Does the State Have a Compelling Interest in Searching Device Data at the Border? Emerging Approaches to Reasonable Search in Canada and the United States

Robert Diab, Associate Professor, Faculty of Law, Thompson Rivers University

[**Print-friendly version** of article in the **Oxford University Comparative Law Forum** 2018]

Abstract: Courts in Canada and the United States currently hold warrantless and groundless device searches at the border to be reasonable. They do so by assuming the state's pressing interest in search at the border extends to the search of device data at the border. Apex courts in both nations have yet to address the issue. Yet in recent cases on device searches on arrest (*Fearon* and *Riley*) both courts have made holdings about privacy and the state interest in device searches that run contrary to assumptions in the border search cases. In the wake of *Fearon* and *Riley*, courts in border cases have conceded the greater privacy in device data but have tended not to question assumptions about the state interest in data search at the border.

This paper examines the development of the law on border device searches in both nations with three aims. The first is to show that governments and courts have not been sufficiently critical of state interest in assessing reasonable border data searches. The second aim is to consolidate critical opinion on the nature of the state's interest in border data searches, and to add the argument that the state has a less pressing interest in data search here than in the search of a person's body, calling for a higher standard than reasonable suspicion. The third aim is to demonstrate that in recent reform efforts in Parliament and Congress, lawmakers have begun to question whether groundless border device searches are reasonable but have lacked clarity on state interest. The paper concludes by suggesting that reasonable search should be assessed in this context by foregrounding the question of state interest and taking an evidence-based approach, and that doing so supports a warrant standard.

Citation:

Robert Diab, "Does the State Have a Compelling Interest in Searching Device Data at the Border? Emerging Approaches to Reasonable Search in Canada and the United States" (2018) Oxford U Comparative L Forum 1 at ouclf.iuscomp.org

Introduction

Customs officials in Canada and the United States have been searching phones and laptops for over a decade.[1] In the past three years, device searches at the US border have risen dramatically.[2] Canadian customs officials have only recently begun to track the number of data searches they conduct, yet public concern is growing.[3] Concerns in both nations focus on the fact that border agencies assert the authority to carry out device searches without reasonable grounds or suspicion.[4] Both governments assume the state's pressing interest in search at the border extends to the search of device data. Courts in both countries have tended to accept this proposition without questioning it. Until recently, courts have also tended to treat border data searches as analogous to cursory bag or pat-down searches, holding groundless searches to be reasonable. The holdings have thus run contrary to case law on digital privacy in other contexts. Apex courts in Canada and the US have yet to address what constitutes a reasonable device search at the border.

The highest courts in both nations have, however, recently decided cases on the search of device data on arrest, and the decisions in each case challenge assumptions at the core of the border device search cases. In 2014, the US Supreme Court in *Riley v California*[5] and the

[1] See discussion below of early case law involving challenges to the constitutional validity of the searches.

[2] US Customs and Border Protection, 'CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics' (cpb.gov, 5 January 2018), noting 30,200 device searches for fiscal year 2017—an increase from 8,503 in 2015, and 19,033 in 2016: <https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and> accessed 3 December 2018. The latter two statistics are found in US Customs and Border Protection, 'CBP Releases Statistics on Electronic Device Searches' (cpb.gov, 11 April 2017) <https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0> accessed 3 December 2018. See also Keveh Waddell, 'The Steady Rise of Digital Border Searches' *The Atlantic* (Boston, 12 April 2017): "the rate of digital border searches is in on pace to quadruple since 2015."

[3] Jim Bronskill 'Canadians Should Worry About US Border Searches of Cell Phones, Electronics: Privacy Czar' *Globe and Mail* (Toronto, 18 September 2017); Matthew Braga, 'What Happens When a Canadian Border Agent Asks to Search Your Phone?' cbc.ca (Toronto, 3 March 2017) <https://www.cbc.ca/news/technology/border-phone-laptop-search-cbsa-canada-cbp-us-1.4002609> accessed 3 December 2018.

[4] The law and government policy on device searches in both countries is canvased in detail in Parts 1 and 2 below.

[5] *Riley v California*, 134 S Ct 2473 (2014) [*Riley*].

Supreme Court of Canada in *R v Fearon*[6] addressed whether police powers to carry out a warrantless search incident to arrest should extend to the search of a digital device. Both Courts held the privacy interest in digital devices to be high.[7] Both Courts also considered whether a search of device data on arrest was connected to, and effective in advancing, state interests in search on arrest. In *Riley*, the Court unanimously declined to find a meaningful connection or a pressing interest. The Court in *Fearon* was divided, with the majority affirming a pressing state interest in search and the dissent taking a more critical view. However, despite the different outcomes, *Riley* and *Fearon* presented a contrast to the case law on device searches at the border in two respects. Courts in both nations had been reluctant to recognize a high privacy interest in the laptops and phones people carry over the border. And courts neglected to question whether the state has a pressing interest in searching device data at the border.

In the wake of *Fearon* and *Riley*, courts in border cases have acknowledged a high privacy interest in device data, but they have failed to engage in a similar critical analysis of state interest.

This paper examines the law and policy debate on border search of device data in both nations to advance three aims. The first aim is to show that courts and governments have taken the view that warrantless data searches here are reasonable without being sufficiently critical of whether the state's interest in searching data at the border is *pressing*. Part I of the paper canvases legislation, border agency guidelines, and case law. It shows that while legislation is ambiguous on data searches, border agencies have asserted a need to carry out warrantless searches based on assumptions about a high state interest that is often asserted as self-evident or claimed without supporting evidence and courts have accepted this reasoning. Part I concludes by arguing that a failure by courts to probe the issue of state interest in border data searches runs contrary to the more balanced approach in *Riley* and *Fearon*.

The paper's second aim, advanced in Part II, is to present a consolidation of critical opinion on the state's interest in border data searches—and to build upon it. Law scholars have been critical of the state interest in data search at the border for over a decade.[8] But litigants and

[6] *R v Fearon*, 2014 SCC 77 [*Fearon*].

[7] Both judgements are examined in more detail in Part I below.

[8] Scholarship on US law is addressed *infra*, notes 156 and 159; on Canada, see Robert Currie, 'Electronic

judges have tended to overlook much of this work, focusing instead on privacy (a topic on which most scholarship on point has also been focused).[9] Part II identifies the two most common arguments in critical scholarship against the claim that the state has a pressing interest in data search at the border. One is the lack of a rational connection of data searches to convention border search purposes or a tenuous connection. The second is the claim that even if such searches are rationally connected, frequent warrantless and groundless searches are disproportionate measures, given the high privacy interest at issue and the questionable effect of the searches. This paper sets out a third argument: the state has a less pressing interest in the search of a device here than in the search of a person's body and thus merits a higher standard than reasonable suspicion.

The paper's third aim, pursued in Part III, is to demonstrate that in recent reform efforts in Parliament and Congress, lawmakers have begun to question whether groundless border device searches are reasonable but have lacked clarity on state interest. Lawmakers are clear in asserting a higher privacy interest in devices but less clear on the nature of the state interest in data searches. This part examines the submissions to, and final report of, a 2017 Parliamentary committee tasked with assessing device searches at airports and borders.[10] The hearings offered privacy advocates and lawmakers an ideal opportunity to undertake a more fulsome analysis of the state's interest in the search of data at the border, and the Committee expressed a clear interest in the issue. Yet participants lacked clarity on state interest and crucial questions failed to be asked—a failure that affects the validity of the Committee's recommendations.

Part III also considers a bill tabled in both houses of Congress in April of 2017, the

---

Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?' (2016) 14(2) CJLT 289; Steven Penney, '"Mere Evidence"? Why Customs Searches of Digital Devices Violate Section 8 of the *Charter*' (2016) 49:1 UBC LR 485; Agathon Fric, 'Reasonableness as Proportionality: Towards a Better Constructive Interpretation of the Law on Searching Computers in Canada' (2016) 21 Appeal 59; Robert Diab, 'Protecting the Right to Privacy in Digital Devices: Reasonable Search on Arrest and at the Border' (2018) 69 UNBLJ 96.

[9] See *eg*, Eunice Parks, 'The Elephant in the Room: What Is a 'Nonroutine' Border Search, Anyway? Digital Device Searches Post-*Riley*' (2017) 44:3 Hastings Const LQ 277 and Currie, *supra* note 8.

[10] Canada, House of Commons, Standing Committee on Access to Information, Privacy and Ethics: *Protecting Canadians' Privacy at the U.S. Border* (December 2017) (Chair: Bob Zimmer).

Protecting Data at the Border Act,[11] requiring a warrant for device searches. The discussion reflects a different set of assumptions about state purposes and reasonable search at the border, but the assumptions should have been made more explicit. The paper concludes by suggesting that reasonable search should be assessed in this context by foregrounding the question of state interest and considering it in light of evidence, and that doing so supports a warrant requirement.

Part I: Reasonable search of device data at the border in Canada and the US

As the law has developed on device searches at the border, governments and courts have taken the view that warrantless data searches are reasonable—and have done so without probing the question of state interest. The decisions in *Riley* and *Fearon* invite this analysis, but it remains exceptional. Tracing these developments lends clarity on the arguments about the state interest that need to be foregrounded for a more effective assessment of what constitutes a reasonable search in this context.

This part deals first with Canada followed by the US, and in each case briefly addresses the law on search at the border, before turning to current law and policy on device searches.

a. Canada

Under section 8 of Canada's *Charter of Rights and Freedoms* "[e]veryone has a right to be secure against unreasonable search or seizure."[12] In *Hunter v Southam*,[13] the Supreme Court held that the purpose of section 8 is to protect a person's reasonable expectation of privacy.[14] In *R v Collins*,[15] the Court held that a search will be reasonable under section 8 if it is authorized by law, the law itself is reasonable, and the search is carried out in a reasonable manner.[16] The question when assessing whether a law that authorizes a search is reasonable depends on whether it strikes an

[11] S 823, HR 1899, 115th Congress.

[12] *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*].

[13] *Hunter v Southam Inc.*, [1984] 2 SCR 145 [*Hunter*].

[14] *Ibid* at 159.

[15] *R v Collins*, [1987] 1 SCR 265.

[16] *Ibid* at 278.

appropriate balance between individual and state interests.[17] A reasonable search generally requires a warrant on probable grounds, but warrantless searches are reasonable in various contexts.[18] In these cases, the state's interest is held to be greater or the individual's privacy interest to be lower, or both.[19] The border is one such context.

Search of persons and goods at the Canadian border

The Canada Border Services Agency (CBSA) is authorized to carry out searches under various acts, including the *Criminal Code*,[20] the *Immigration and Refugee Protection Act*,[21] and the *Customs Act*.[22] The CBSA relies most often on *Customs Act* provisions allowing for cursory search of goods without reasonable grounds, or more invasive searches of persons and goods on reasonable suspicion.[23] The common law lends essential context for understanding how the CBSA

[17] *Hunter*, *supra* note 13, 167-8: "The state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement. Where the state's interest is not simply law enforcement as, for instance, where state security is involved, or where the individual's interest is not simply his expectation of privacy as, for instance, when the search threatens his bodily integrity, the relevant standard might well be a different one."

[18] *Ibid*, 159; 167-8. Reasonable exceptions to the warrant requirement include search incident to arrest: *Cloutier v Langlois*, [1990] 1 SCR 158 [*Cloutier*]; search incident to investigative detention: *R v Mann*, 2004 SCC 52; the use of sniffer dogs in certain public spaces: *R v Kang-Brown*, 2008 SCC 18; and the search of lockers in schools: *R v M(MR)*, [1998] 3 SCR 393.

[19] In the context of arrest, for example, the state interest in safety and evidence discovery or preservation outweighs a person's privacy interest: *R v Caslake*, [1998] 1 SCR 51 [*Caslake*], para 17; and *Fearon*, *supra* note 6, para 45.

[20] RSC 1985, c C-46.

[21] SC 2001, c 27 [*IRPA*].

[22] RSC, 1985, c 1 [*Customs Act*].

[23] For cursory searches, the CBSA relies on section 99(1)(a), which allows an officer to "examine any goods that have been imported" and section 99.3(1) permits a "non-intrusive examination of goods" in "custody or possession" of a person in a "customs controlled area" (CCA). The latter area is a space in an airport or port designated by regulation. The *Customs Act* was amended in 2001 and in 2009 to allow for the designation and implementation of a CCA to address concerns about airport staff colluding with organized crime in illicit conduct. Several CCAs been designated thus far: see the list at <https://www.cbsa-asfc.gc.ca/security-securite/cca-zcd/menu-cca-zcd-eng.html> accessed 3 December 2018 (the list includes areas in all of Canada's major airports). For context on the addition of CCAs in the *Customs Act*, see the "Regulatory Impact Analysis Statement" which appears as a schedule to the *Customs Controlled Areas Regulations*, SOR/2013-127. More invasive searches can be conducted of persons on reasonable suspicion under section 98(1) and of goods under section 99(1)(c.1) to (f). Steven Penney

and courts interpret these provisions in relation to data searches.

The leading authority on search at the border is the Supreme Court's decision in *R v Simmons*,[24] which dealt with a *Charter* challenge to strip search powers in an earlier version of the *Customs Act*. Dickson CJ held that "degree of personal privacy reasonably expected at customs is lower than in most other situations" – where we anticipate "scrutiny" and accept that "sovereign states have the right to control both who and what enters their boundaries".[25] Drawing on US jurisprudence, he held that "border searches lacking prior authorization and based on a standard lower than probable cause are justified by the national interests of sovereign states in preventing the entry of undesirable persons and prohibited goods, and in protecting tariff revenue."[26]

Chief Justice Dickson then set out three categories or "types" of border search within which the validity search powers are to be assessed—a scheme that is relevant to later case law on electronic devices:

> 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,

points out that "[t]here does not seem to be any statutory authority…to frisk without reasonable suspicion. It also appears that no court has recognized a common law authority to do so." Penney, *supra* note 8, at 510.

[24] [1988] 2 SCR 495 [*Simmons*].

[25] *Ibid*, para 48.

[26] *Ibid*.

and to other highly invasive means.[27]

Simmons dealt with a search of the second type.[28] The Court held that a power authorizing strip searches on reasonable suspicion constitutes a reasonable search under section 8 due to both compelling state interests and key protections. The state has a compelling need to carry out strip searches not only pursuant to a broad interest in enforcing customs laws, but more specifically, "[i]n light of the existing problems in controlling illicit narcotics".[29] The state interest in strip search *per se* was therefore not merely speculative or theoretical but grounded in evidence and experience.

Later courts have added important qualifications to the *Simmons* framework. The Ontario Court of Appeal in *R v Hudson*[30] held that the *Simmons* schema entails "discrete categories and not a continuum"—requiring a decision about classification before deciding on the "level of constitutional protection engaged."[31] Courts have made clear that searches do not belong in the second category in *Simmons* by virtue of taking place at a remove from the main passageway in a border area, or being a 'secondary search.'[32] Case law on the scope of a category 1 search in *Simmons* indicates that it includes a cursory search of baggage or purses, pockets, and the tapping

---

[27] *Ibid*, para 27. Chief Justice Dickson's comment that "no constitutional issues are raised" by a search of the first type has been the source of confusion and disagreement among lower courts as to whether a person has a reasonable expectation of privacy at the first stage. (See *eg*, *R v Jones*, [2006] OJ No 5464 (Ont CA), holding there to be no REP at stage 1, and *R v Nagle*, 2012 BCCA 373, applying a section 8 analysis to a stage 1 search.) Robert Currie, *supra* note 8, 302, suggests that Dickson CJ meant here that no issue is raised in terms of detention. Currie also notes that the passage pre-dates the Court's framework for a section 8 analysis, beginning with *R v Edwards* [1996] 1 SCR 128, in which REP is determined as a threshold question for section 8. See also Penney, *supra*, note 8, 501.

[28] *Simmons*, *supra* note 24, para 28; Dickson CJ added a proviso here with respect to the other categories: "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."

[29] *Ibid*, para 52.

[30] 2005 CanLII 47233 ON CA [*Hudson*].

[31] *Ibid*, para 30.

[32] *Dehghani v. Canada (Minister of Employment and Immigration)*, [1993] 1 SCR 1053, 1073.

of exterior parts of a car or truck to detect a hidden compartment.[33]

Search of device data at the Canadian border

The CBSA claims authority to search a device and its data under sections 99(1)(a) and 99.3(1) of the *Customs Act*.[34] Section 99(1)(a), the most commonly invoked, allows an officer to "examine any goods that have been imported", while section 99.3(1) permits a "non-intrusive examination of goods" in the "custody or possession" of a person in a "customs controlled area".[35] Section 2 of the Act defines "goods" to include "any document in any form", and the CBSA takes the position that data on a device is a "document."[36] A number of trial courts across Canada have agreed, holding section 99(1)(a) or 99.3(1) to be sufficient authority for a device search.[37] As a result, when CBSA officials search data on a device, they do so without any limits imposed by the Act, aside from the vague requirement that the search be "non-invasive" if performed pursuant to

[33] *Hudson*, *supra*, note 30; *R v Sekhon*, 2009 BCCA 187.

[34] *Customs Act*, *supra*, note 22.

[35] *Ibid*.

[36] Canada Border Services Agency, "Operational Bulletin: PRG-2015-31" (30 June 2015) ["Guidelines"]. The British Columbia Civil Liberties Association made the Guidelines public in August of 2016, after obtaining them through an access to information request. The Ministry of Public Safety confirmed their currency in February of 2017, as did Martin Bolduc, Vice-President of CBSA's Programs Branch in submissions to Parliament in September of 2017, discussed further below. See Michael Vonn, 'What Happens If You Don't Provide Your Cellphone Password to Border Agents?' British Columbia Civil Liberties Association (Vancouver, 25 August 2016) <https://bccla.org/2016/08/what-happens-if-you-dont-provide-your-cellphone-password-to-border-agents/> accessed 3 December 2018; Matthew Braga, 'Canadian Policies on Cellphone Searches at Border Aren't Easy to Find' CBC News (Toronto, 17 February 2017) <https://www.cbc.ca/news/technology/cbsa-border-smartphone-laptop-electronic-device-search-policy-1.3986496> accessed 3 December 2018, and Matthew Braga, 'Canada's Border Agency to Start Tracking the Number of Cellphone Searches' CBC News (Toronto, 28 September 2017) <https://www.cbc.ca/news/technology/cbsa-border-agency-cellphone-searches-tracking-statistics-1.4311830> accessed 3 December 2018. A more recent but amended version can be found online; the text cited above is from the earlier version published by the BCCLA, beginning at page 3: <https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf> accessed 3 December 2018.

[37] *R v Canfield*, 2018 ABQB 408, para 52 [*Canfield*]; *R v Gibson*, 2017 BCPC 237, para 94-98 [*Gibson*]; *R v Buss*, 2014 BCPC 16 [*Buss*], paras 25-31; *R v Moroz*, 2012 ONSC 5642 paras 20-22 [*Moroz*]; and *R v Saikaley*, 2012 ONSC 6794, paras 79-82 [*Saikaley*]; *R v Whittaker*, 2010 NBPC 32, para 8; *R v Mozo*, 2010 CanLII 96558 (NL PC), para 34; and *R v Leask*, 2008 ONCJ 25, para 7 and note 3 of the decision. In all of these cases aside from *Mozo*, the only authority cited is section 99(1)(a). In *Mozo*, both 99(1)(a) and 99.3(1) were held to be adequate authority.

99.3(1) (which applies only in a 'customs controlled area').[38] Courts have held device searches under these provisions to be a category 1 search in *Simmons*, no different in essence from an officer glancing inside a bag or purse.[39]

A set of Guidelines the CBSA circulated in 2015 state that the Agency searches data to obtain "information that may afford evidence to [*sic*] a contravention of CBSA-mandated legislation that governs the admissibility of people and goods, plants and animals into and out of Canada".[40] This might include "a confirmation of identity; receipts and invoices for imported goods; contraband smuggling; or, the importation of obscenity, hate propaganda or child pornography."[41] The Guidelines also indicate that:

> [a]lthough there is no defined threshold for grounds to examine [digital] devices, CBSA's current policy is that such examinations should not be conducted as a matter of routine; they may only be conducted if there is a *multiplicity of indicators* that evidence of contraventions *may* be found on the digital device or media.[42] [emphasis added]

A "multiplicity of indicators" authorizes "progressive examinations of digital devices".[43] The Guidelines require that a search "always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation"[44] and that "the officer's notes shall clearly articulate the types of data examined, and their reason for doing so."[45] Officers should disable wireless radios on a device before proceeding to search, and if a traveler refuses a password, the device may be detained under the *Customs Act*.[46] The officers are advised that "[u]ntil further

[38] The decision of the British Columbia Provincial Court in *R v Gibson*, *ibid*, holds to the contrary, finding certain implied limits in the *Customs Act* discussed below.

[39] See *eg Buss*, *supra*, note 37, para 30; *Gibson*, *supra*, note 37, para 198.

[40] *Supra*, note 36, 2.

[41] *Ibid*, 2.

[42] *Supra*, note 36, 1.

[43] *Ibid*.

[44] *Ibid*, 1-2.

[45] *Ibid*, 2.

[46] *Ibid*, 3 and 4, citing section 101 of the Act, *supra* note 22, for authority to detain goods until an officer is "satisfied that the goods have been dealt with in accordance with this Act".

instructions are issued," they are not to arrest a traveler for refusing.[47]

Canadian case law on border device searches

The body of cases in Canada on device searches at the border is relatively small.[48] But patterns can be discerned. With one exception, all are trial-level decisions. The search in 8 of the 11 cases uncovered child pornography.[49] In all but one case (*Gibson*, 2017), courts were reluctant to recognize that 'digital is different,' or that device data engages a high privacy interest.[50] None of the cases refer to the Guidelines noted above, or analogous material. And none of the cases, including *Gibson*, contains a discussion of whether the state's interests in search at the border meaningfully extends to the search of data on devices. The pattern of reasoning here is problematic on two grounds.

First, the failure in all but the most recent of these cases to recognize the high privacy interest in device data stands in tension with emerging jurisprudence on digital privacy. In a

[47] The passage setting out purported authority for this appears at 4, *ibid*: "Until further instructions are issued, CBSA officers shall not arrest a traveller for hindering (Section 153.1 of the *Customs Act*) or for obstruction (paragraph 129(1)(d) of *IRPA*) solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings."

[48] There are, to my knowledge, eleven reported decisions involving device searches at the border. Including the eight cases listed in note 37 *supra*, three additional cases are *R v Bares*, 2008 CanLII 9367 (ON SC) (involving the search of CDs rather than a device); *R v Appleton*, 97 WCB (2d) 444 (2011) (ONCJ) [*Appleton*]; and *R v Bialski*, 2018 SKCA 71 [*Bialski*] (a decision not squarely on point, but affirming the trial court's holding that the device search in this case, pursuant to section 99 of the *Customs Act*, was not an unreasonable search, or if it did violate section 8, the evidence would have been admitted under section 24(2) of the *Charter*). I note that this list is consistent with Robert Currie's inventory, *supra* note 8 at 300, with the addition of the more recent *R v Gibson*, *supra* note 37 and *Bailsky*.

[49] The two other cases are *Appleton*, *ibid*, and *Saikaley*, *supra*, note 37. The search in *Appleton* involved a text message. In *Saikaley*, CBSA recover a debt list from a suspected drug-dealer's phone but were acting on information gleaned from a wiretap and an earlier investigation by the RCMP.

[50] See *eg*, *R v Leask*, *supra* note 37, Justice Nadel holding: "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." Notably, both of the latter decisions pertain to devices that pre-date the advent of the smart-phone. See also *R v. Saikaley*, *supra* note 37, paras 92 to 94, and *Canfield*, *supra* note 37, in which Justice Belzil dismisses the argument, paras 34-35 that in the wake of *Fearon*, supra note 6, a device search is closer in nature to a strip search.

series of cases, from *R v Morelli*[51] onward, including *R v Vu*[52] and *R v Fearon*,[53] the Supreme Court has held that digital devices engage a high expectation of privacy.[54] As Fish J wrote in *Morelli*, "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer".[55] The Court's decision in *Vu* contained an extended discussion of the distinct qualities of digital devices that engage a higher privacy interest, decisively settling the question of whether 'digital is different'.[56]

Thus, as Robert Currie has pointed out, trial courts have failed to effectively reconcile the Supreme Court's recognition of a heightened privacy interest in computers, or their distinctness from physical containers, and the allowance in *Simmons* for cursory searches without grounds.[57] Arguments among defence counsel to the effect that the higher privacy interest calls for reasonable grounds to one standard or another have fallen flat.[58] So too have concerns about groundless and limitless searches failing to perform the prophylactic function noted in *Hunter v Southam*[59] of avoiding unnecessary breaches before they occur.

A second problematic aspect of the pattern of reasoning in the border device cases

---

[51] *R v Morelli*, 2010 SCC 8 [*Morelli*].

[52] *R v Vu*, 2013 SCC 60 [*Vu*].

[53] *Fearon*, *supra* note 6.

[54] The most extensive discussion is set out in *Vu*, *supra* note 52, paras 40-45; see also *Morelli*, *supra* note 51 paras 1 and 105-106; *R v Cole*, 2012 SCC 34, paras 47-49; and *R v Spencer*, 2014 SCC 43, para 50.

[55] *Morelli*, *supra* note 51, para 2. Justice Karakatsanis, in *Fearon*, *supra* note 6, writing at para 152 in dissent, but not on this point: "[a] modern digital device is a portal to vast stores of information that are not truly on the device, and digital information has the potential to be more intensely and extensively personal than what might be found in a briefcase. Particularly for the 'digital generation', these devices contain far more information, and information far more personal, than does a private home."

[56] *Vu*, *supra* note 55, paras 41-44. Cromwell J summarized this discussion at para 51 of *Fearon*, *supra* note 6: "As outlined in *Vu*, computers — and I would add cell phones — may have immense storage capacity, may generate information about intimate details of the user's interests, habits and identity without the knowledge or intent of the user, may retain information even after the user thinks that it has been destroyed, and may provide access to information that is in no meaningful sense "at" the location of the search".

[57] This would include *Moroz*, *Sakaley*, *Buss*, and *Gibson*, all *supra* note 37. Robert Currie, *supra* note 8, 306.

[58] See *eg* the two post-*Vu* decisions of the BC Provincial Court in *Buss* and *Gibson*, *supra* note 37.

[59] *Hunter*, *supra* note 13.

involves the court's failure to question whether the state interest in the search of digital devices is pressing—or whether the logic in *Simmons* should also apply to the search of device *data*. In all but the most recent cases, courts have entirely overlooked the question of whether the state has a compelling interest in data searches at the border, and if so, what evidence supports this. Courts have instead employed a narrow pattern of reasoning that begins by finding that data is a "good" under the *Customs Act* (relying on earlier authority predating the smart phone), and then holding the search to fall within category 1, requiring no grounds.[60] *Gibson* marks a partial break with this pattern. The court in this case sought to reconcile earlier search authority with the Supreme Court's holdings in *Vu* and *Fearon*. Before turning to *Gibson*, it would be helpful to consider *Fearon* briefly, given its broader relevance in this context.

R v Fearon

Fearon addressed whether the common-law power of search incident to arrest, which requires neither a warrant nor additional grounds, should extend to the search of data on a device.[61] In the wake of its holding in *Vu*, the Court had given rise to an expectation that it would require a warrant for the search of device data on arrest, as did the United States Supreme Court earlier in 2014 in *Riley v California*.[62] However, in a 4-3 decision, the majority of Canada's Supreme Court held that a cursory search of device data is reasonable on certain conditions.[63]

Writing for the majority, Cromwell J affirmed the Court's earlier holding in *Vu* that devices engage a high privacy interest, but also held that "while cell phone searches...may constitute very significant intrusions of privacy, not every search is inevitably a significant intrusion."[64] His Lordship also held that the search of a phone is "completely different" from a strip search, which is "invariably and inherently… a significant affront to human dignity."[65]

---

[60] Commonly cited for this proposition are the Ontario Court of Justice's 2008 decision in *Leask*, *supra* note 39, and the Ontario Superior Court of Justice's 2012 decision in *Moroz*, *supra*, note 37.

[61] The Court had recognized the power of search incident to arrest in *Cloutier*, *supra* note 18 and *Caslake*, *supra* note 19.

[62] *Supra* note 5.

[63] *Fearon*, *supra* note 6, para 83.

[64] *Ibid*, para 54.

[65] *Ibid* para 55.

Justices Karakatsanis, LeBel, and Abella, in dissent, held the invasion to be comparable to a strip search or the search of a home.[66] The dissent also held that "it is very difficult — if not impossible — to perform a meaningfully constrained targeted or cursory inspection of a cell phone or other personal digital device."[67] In their view, a warrantless search, except in exigent circumstances, would be unreasonable.

A more crucial difference of opinion in *Fearon* related to the assessment of the state interest in the search of a device. The majority held the state interest in immediate access to device data on arrest was pressing because devices could be used to notify parties to an offence of police involvement, potentially endangering police, or evidence might be remotely destroyed.[68] The dissent considered the issue at greater length and took a more skeptical view.[69] Devices may in theory be used to "summon violent backup", or be wiped remotely, but both occurrences are likely to be rare and best dealt with under an exigent circumstances exception.[70] In most cases, information will remain on the device while police seek a warrant, as would have been the case in *Fearon* itself.[71] "The mere *possibility* that evidence on the cell phone could be remotely deleted should not justify a search."[72] Similarly, concerns about the use of a device to reach an accomplice can be addressed through a 'Faraday bag' or other such technique.[73] Finally, device data may in some cases help police locate accomplices and for this speed is important, but even here, police should either obtain a tele-warrant or rely on the exigent circumstances exception.[74]

---

[66] *Ibid*, para 101 and 152: "These devices provide a window not just into the owner's most intimate actions and communications, but into his mind, demonstrating private, even uncommunicated, interests, thoughts and feelings. Thus, like the search of the body and of the home, the warrantless search of personal digital devices as an incident of arrest is not proportionate to our privacy interests."

[67] *Ibid*, para 164.

[68] *Ibid*, paras 46-49. In *Fearon* itself, police discovered a photo of a weapon used in the robbery at issue that had yet to be recovered.

[69] *Ibid*, paras 135-150.

[70] *Ibid*, paras 140-143.

[71] *Ibid*, para 144.

[72] *Ibid*.

[73] *Ibid*.

[74] *Ibid*, paras 147 and 150.

Fearon offered a broader lesson that extends to the border context. To assess whether a law authorizing the search of a digital device is reasonable, courts should carefully consider both the degree of privacy at issue *and* the nature of the state's interest in a search of this kind. In *Fearon*, the Court had a small difference of opinion on the privacy issue but a major difference on the state purpose issue. Both the majority and dissent agreed that a search of device data incident to arrest is rationally connected to the purposes of the arrest search exception to the warrant requirement: safety and the discovery and preservation of evidence.[75] Yet, for the majority, a *potential* usefulness sufficed to support a view that the state has a compelling interest in search of this nature. For the dissent, the lack of evidence that data searches advance valid purposes with any frequency suggested that aside from exceptional cases, the state does not have a compelling interest in data search on arrest. Regardless of this difference, however, the larger point bears emphasis: assessing reasonableness requires a distinct inquiry into state interest.

Fearon's relevance at the border?

In the wake of *Fearon*, Canadian courts in border device search cases should have begun to engage in a more careful assessment of *both* the privacy and state interests at issue. The British Columbia Provincial Court decision in *Gibson* stands out from earlier border cases by considering *Fearon*'s holdings on privacy, but simply assumed the state interest in both cases is analogous.[76] Searching a phone on arrest, police may find further evidence of the crime for which a person is arrested, but customs officials aim to prevent illegal entry of persons and things into Canada. Courts trying to assess whether customs officials have a pressing need for immediate access to device data should do so by considering the kinds of evidence border device searches tend to uncover, and how often such evidence is uncovered in relation to the number of searches carried out. The debate between the majority and dissent in *Fearon* compelled this analysis, and without it, the assertion that the state has an analogous interest in data search in the two contexts

[75] These purposes were canvassed in *Cloutier*, *supra* note 18, to be safety and the discovery or preservation of evidence.

[76] *Ibid*, para 179: "parallels exist between the exigencies of law enforcement in having timely access to cellular telephones and Customs officers undertaking timely examinations of individuals and their goods at the border".

is questionable.

In summary, customs legislation in Canada is unclear on how to treat device searches. The CBSA and Crown have taken the view that, since device data are "goods" under the *Customs Act*, the law authorizes device searches as routine, falling within category 1 in *Simmons*, and thus without a warrant or reasonable grounds. Canadian courts have begun to challenge the government's view that device searches are no more invasive than a baggage or pat-down search—however, they have yet to follow *Fearon*'s lead in questioning the state interest in device searches and engaging in a more effective balancing of interests on which an assessment of reasonable search is premised. Before turning to the question of state interest in more detail, I turn next to the United States, to demonstrate a similar evolution of the law.

b. Border device searches in the United States

Prior to 1967, US courts had held the Fourth Amendment's guarantee against unreasonable search[77] to protect places or personal effects.[78] In *Katz v US*,[79] the Supreme Court held that the guarantee applies more broadly to protect a person's "reasonable expectation of privacy" in a given situation.[80] A reasonable search requires a warrant on probable cause, and although warrantless searches "are per se unreasonable",[81] courts have recognized as reasonable a number of exceptions to this standard.[82] In these cases, courts have recognized a law authorizing a search on a lower standard to be reasonable in light of a lower privacy interest or a more pressing state interest, or both.[83]

---

[77] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches or seizures." US Const, amend IV.

[78] *Olmstead v United States*, 277 US 438 (1928); *Goldman v United States*, 316 US 129 (1942).

[79] *Katz v United States*, 389 US 347 (1967) [*Katz*].

[80] *Ibid* at 360.

[81] *Ibid* at 357.

[82] These include a pat-down search incident to investigatory detention, a search incident to arrest, and search under exigent circumstances: *Terry v Ohio*, 392 US 1; *United States v Robinson*, 414 US 218; and *Warden, Md. Penitentiary v Hayden*, 387 US 294.

[83] *Wyoming v Houghton*, 526 US 295: holding at 300 that the reasonableness of a warrantless search is determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental

Search of persons and goods at the US border

The power to carry out a warrantless search at the border is an example of this—one as old as the Fourth Amendment itself.[84] Courts have long held the state interest in search at the border to be high and the personal expectation of privacy to be low.[85] But the assessment and scope of a reasonable search here is closely tied to the purposes for which it is carried out.[86] A primary purpose is to enforce importing and exporting laws, and to ensure that duties are being paid.[87] Another key purpose is to identify the persons attempting to enter the country, their entitlement to enter, and to lawfully bring in their effects.[88] A border search is thus reasonable so long as it is tied to a legislative mandate to police the border, rather than to gather evidence for ordinary crime.[89] The power of search at the border on a lower standard is not meant to give law

interests". See also *Terry v Ohio*, *ibid*, 20-24.

[84] *United States v Ramsey*, 431 US 606 [*Ramsey*], 616: "That searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border should, by now, require no extended demonstration. The Congress which proposed the Bill of Rights, including the Fourth Amendment, to the state legislatures on September 2, 1789, 1 Stat. 97, had, some two months prior to that proposal, enacted the first customs statute, Act of July 31, 1789, c. 5, 1 Stat. 29. Section 24 of this statute granted customs officials 'full power and authority' to enter and search 'any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed. …' This acknowledgment of plenary customs power was differentiated from the more limited power to enter and search 'any particular dwelling-house, store, building, or other place . . .' where a warrant upon 'cause to suspect' was required."

[85] *Carroll v US*, 267 US 132 (1925) [*Carroll*] at 154; *United States v. Montoya de Hernandez*, 473 US 531 (1985) [*Hernandez*] 539-40: "not only is the expectation of privacy less at the border than in the interior […] the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border."

[86] *Ramsey*, *supra*, note 90, 616.

[87] *Boyd v United States*, 116 US 616 (1886) [*Boyd*], 623; customs legislation "authoriz[es] the examination of ships and vessels, and persons found therein, for the purpose of finding goods prohibited to be imported or exported, or on which the duties were not paid, and to enter into and search any suspected vaults, cellars, or warehouses for such goods."

[88] *Carroll*, *supra*, note 91, 154: "Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."

[89] *Boyd*, *supra* note 93, 623; see also *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000), holding an Indianapolis' check-point program to violate the Fourth Amendment because its primary purpose went beyond the regulation of highway traffic to "the general interest in crime control".

enforcement a space in which they might circumvent ordinary procedural protections.[90]

In the post-*Katz* era, the Supreme Court has made three decisions that shed further light on the scope of the 'border search exception' to the warrant requirement. In *United States v Ramsey* (1977),[91] the Court held that a cursory search of persons and goods at the border does not require a warrant or probable grounds.[92] It also held that a border official's search of the content of international mail on reasonable suspicion that it contained contraband was reasonable.[93] An important limitation here was that reading any *correspondence* contained in a piece of mail still requires a warrant.[94]

In *United States v Montoya de Hernandez* (1985),[95] the Court recognized a distinction between 'routine' and more invasive 'non-routine' searches.[96] The lower expectation of privacy at the border and heightened state interest in search renders routine searches of persons and goods reasonable without grounds.[97] The Court also held that travelers could be detained and strip searched on reasonable suspicion of smuggling.[98] In *United States v Flores-Montano* (2004),[99] the Court held that the removal and dismantling of a vehicle gas tank was a 'routine' search,

---

[90] *United States v Seljan*, 547 F3d 993 (9th Cir 2008), 1015: "…the purpose of all these searches is the interdiction of prohibited or dutiable items concealed within the package that is crossing the border. Using border searches for a purpose unrelated to border control—such as general crime prevention—raises a wholly different issue. […] [I]n *United States v. Bulacan*, we reiterated that 'courts must take care to ensure that [a suspicionless contraband] search is not subverted into a general search for evidence of crime,' emphasizing the 'vast potential for abuse' and intrusion 'into the privacy of ordinary citizens.' 156 F.3d 963, 967 (9th Cir.1998)."

[91] *Ramsey*, *supra* note 84.

[92] *Ibid*, 619.

[93] *Ibid*, 623-625.

[94] *Ibid*, 624: "the reading of any correspondence inside the envelopes is forbidden. Any 'chill' [of free expression rights] that might exist under circumstances may fairly be considered not only 'minimal'… but also wholly subjective."

[95] *Hernandez*, *supra* note 85, 540-541.

[96] *Ibid*, 538.

[97] *Ibid*, summarizing the Court's holding in *Ramsey*, *supra*, note 90: "Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant".

[98] *Ibid*, 541.

[99] *United States v Flores-Montano*, 541 US 149 (2004) [*Flores-Montano*].

requiring no grounds. The Court declined to accept an analogy between the dismantling of property and the indignity of a strip search.[100] Lower courts have held that whether a search is routine depends not on the place or thing searched but on the extent of its intrusiveness.[101]

Search of device data at the US border

Immigration law authorizes US border officials to carry out searches to ascertain identity and admissibility.[102] Customs legislation authorizes searches to enforce duties and prevent contraband from entering.[103] The government relies on these provisions as authority to search device data.[104]

In 2009, the US Customs and Border Protection (CBP) published a directive setting out its policy and practices on "border search of electronic devices",[105] and its objectives. The directive asserts that data searches are "essential to enforcing the law at the U.S. border," because they

> …help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations. Finally searches at the border are often integral to a determination of admissibility under the immigration laws.[106]

A substantially similar text appears at the outset of an updated version of the directive published

[100] *Ibid*, 152: "…the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles. Complex balancing tests to determine what is a "routine" search of a vehicle, as opposed to a more "intrusive" search of a person, have no place in border searches of vehicles."

[101] *United States v Irving*, 452 F3d 110 (2d Cir. 2006), 123: "[T]he level of intrusion into a person's privacy is what determines whether a border search is routine"; cited in Miller, *infra*, note 117, 1959.

[102] 8 U.S. Code § 1357 - Powers of immigration officers and employees.

[103] 8 U.S. Code § 1225 - Inspection by immigration officers.

[104] United States Customs and Border Protection, "Border Search of Electronic Devices Containing Information" (Department of Homeland Security: 20 August 2009) [CBP 2009 Directive] at 2 <https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf> accessed 3 December 2018.

[105] CBP 2009 Directive, *ibid*.

[106] *Ibid*, at 1.

in 2018.[107] In outlining the procedure for officers to follow, the directive sets out the agency's view that data searches are comparable in law to cursory searches of bags or compartments, not requiring grounds. Similar to the CBSA Guidelines discussed above, the CBP directive outlines a process for escalating levels of search, documenting steps taken, and seizing a device if locked and a password is not provided.[108]

US case law on border device searches

Courts in early cases on device searches accepted the CBP's interpretation of device search powers. Judges tended to dismiss the distinction between a device and a physical receptacle such as a purse or a brief case, and considered a data search to be "routine," requiring no grounds.[109] In light of this approach, none of the early appellate decisions probed the question of whether the state has a pressing interest in the search of data at the border.[110]

The 2013 decision of the Court of Appeal for the Ninth Circuit in *United States v*

[107] United States Customs and Border Protection, "Border Search of Electronic Devices" (Department of Homeland Security, 4 January 2018) at 1 <https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf> accessed 3 December 2018.

[108] The CBP's border device search policy is summarized in Adam Schwartz et al, 'Digital Privacy at the U.S. Border' Electronic Frontier Foundation (San Francisco, December 2017) 35-40 <https://www.eff.org/document/digital-privacy-us-border> accessed 3 December 2018.

[109] *United States v Arnold*, 533 F3d 1003 (9th Cir 2008), 1009: "Arnold has failed to distinguish how the search of his laptop and its electronic contents is logically any different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed". See also *United States v Linarez-Delgado*, 259 F App'x 506 (3d Cir 2007); *United States v Romm*, 455 F3d 990 (9th Cir 2006); and *United States v Ickes*, 393 F3d 501 (4th Cir 2005).

[110] See, *eg*, *Arnold*, *ibid*, 1006-1007 and *Romm*, *ibid*, 997. The courts in both passages cite *Ramsey*, *supra* note 90, 616, and *Flores-Montano*, *supra* note 99, 152-3 on the sovereign's "paramount" interest in search to protect the border with no consideration of a connection between border protection and data searches. *Ickes*, *ibid*, 506 offers a partial exception. The appellant in that case argued that the search of device data was "invalid since it involved the search of expressive material". The Court dismissed this argument on the view that "The border search doctrine is justified by the 'long-standing right of the sovereign to protect itself.' … Particularly in today's world, national security interests may require uncovering terrorist communications, which are inherently 'expressive.' Following Ickes's logic would create a sanctuary at the border for all expressive material—even for terrorist plans. This would undermine the compelling reasons that lie at the very heart of the border search doctrine." (Citations omitted.) Aside from asserting the proposition that the state has a *compelling* interest in data search here due to the possibility of discovering terrorist plans, the issue is probed no further.

Cotterman[111] marked a partial break with this line of authority by recognizing that people have a high privacy interest in device data, even at the border.[112] The court distinguished between "forensic" searches ('data dumps'), which require reasonable suspicion, and limited "manual" searches, which do not.[113] Yet the court's analysis focused primarily on privacy and neglected to question the state's interest in the search of data at the border.[114] *Cotterman*'s affirmation that groundless data searches at the border are constitutional—despite the high privacy interest at issue—is thus premised on an unquestioned view of the state's pressing interest in immediate access to data. Other courts have followed this reasoning.[115]

However, in 2014, the US Supreme Court decided *Riley v California*,[116] a case dealing with the power to search a phone on arrest, and the Court's approach to device data in that case

---

[111] *US v Cotterman*, 709 F3d 952 (9th Cir 2013).

[112] *Ibid*, 966: "[T]he uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property." At 964: "The nature of the contents of electronic devices differs from that of luggage… [They] are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails."

[113] *Ibid*, 981. The "forensic search" here involved copying the entire content of a laptop hard drive, after confiscating it and conducting a search some 170 miles away: *ibid*, 958.

[114] *Ibid*; the majority referred broadly, at 957, to the "heavy burden on law enforcement to protect our borders", and at 966 to the "important security concerns that prevail at the border", including "terrorism and future threats yet to take shape." But it neglected to consider whether and how often data search advances these purposes. The closest the majority came to recognizing a need to question the extent of the state's interest in the search of *data* in light of effectiveness was in a comment made in passing at 966: "The effort to interdict child pornography is also a legitimate one. But legitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information. Reasonable suspicion is a modest, workable standard that is already applied in the extended border search, Terry stop, and other contexts. Its application to the forensic examination here will not impede law enforcement's ability to monitor and secure our borders or to conduct appropriate searches of electronic devices."

The dissenting opinion was also premised on unsupported assertions. In Smith J's view, at 984, the majority's decision to "insulate electronic devices from search … creates serious national security concerns." To bolster this proposition, the opinion cites the 2009 Customs and Border Protection Directive, noted above, for the assertion that data searches are "essential… [for] "detecting[ing] evidence relating to terrorism and other national security matters"—an assertion not substantiated in the Directive itself (985, citing CBP 2009 Directive, *supra* note 143, 1).

[115] *US v Kolsuz*, 185 F Supp 3d 843, 858 (ED Va 2016); *US v Saboonchi*, 990 F Supp 2d 536 (D Md 2014) 547-48.

[116] *Riley*, *supra* note 5, 2489-91.

presented a clear contrast to the approach in the border search cases. The Court in *Riley* examined at some length not only the privacy interest in device data, but also whether search on arrest bore a rational connection to conventional state purposes for search on arrest and whether it advanced them effectively. In light of all three considerations, the Court held that a reasonable data search on arrest requires a warrant, except in exigent circumstances. Later commentators have argued that the reasoning in *Riley* is applicable to device searches in all contexts including the border,[117] and courts in later device search cases have begun to debate *Riley*'s potential import.[118] Before turning to those cases, *Riley* merits a brief overview.

Riley v California

Riley dealt with companion cases in which phones were searched on arrest. On behalf of a unanimous Court, Chief Justice Roberts began by noting that the arrest search exception to the warrant requirement is generally justified on the basis of a lower privacy interest on arrest and compelling state interests in officer safety and evidence preservation.[119] Yet in the Court's view, the police do not effectively advance these purposes when they search data on arrest.[120] The information contained on a device "cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape".[121] The Court conceded a "strong interest in warning officers" about the possibility of parties to the offence heading to the scene, but noted that "neither the United States nor California offers evidence to suggest that their concerns are based

[117] Thomas Mann Miller, 'Digital Border Searches After *Riley v California*' (2015) 90 Wash L R 1943, 1947; and Adam Schwartz et al, 'Digital Privacy at the U.S. Border' *supra* note 108, 26.

[118] See discussion of *US v Saboonchi* and *United States v Molina-Isodoro* below.

[119] *Riley*, *supra* note 5, 2484, citing *Chimel v. California*, 395 US 752.

[120] *Riley*, *supra* note 5, 2484-85: "[W]hile *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones. On the government interest side, *Robinson* concluded that the two risks identified in *Chimel*—harm to officers and destruction of evidence—are present in all custodial arrests. There are no comparable risks when the search is of digital data. In addition, *Robinson* regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*. We therefore decline to extend *Robinson* to searches of data on cell phones…"

[121] *Ibid*, 2485.

on actual experience."[122] Such concerns are better addressed through the exigent circumstances exception to a warrant requirement.[123] Similarly, while phones might be wiped remotely or used to conceal evidence, the Court held there was no evidence that "either problem is prevalent or that the opportunity to perform a search incident to arrest would be an effective solution."[124]

Equally important, however, was the Court's view of the privacy interest at issue. A person may have a lower expectation of privacy on arrest generally, but they retain a high privacy interest in their data for reasons to do with the "immense storage capacity" of current devices.[125] The Court drew a categorical distinction between digital devices and physical receptacles, settling the question of whether 'digital is different.' In contrast to the kinds of information one would tend to carry in physical documents, a device contains many types of information (addresses, notes, videos), in a larger volume, and often dating back many years. There is also "an element of pervasiveness" about personal devices, with virtually everyone carrying one at all times, which is not the case with "physical records."[126] The privacy interest in devices is further implicated by the possible connection of any device searched with data stored in the cloud—vastly extending the possible scope of a search beyond the immediate vicinity of a person's arrest.[127] The privacy interest in devices is therefore distinct, very high, and closer in nature to the search of a home.[128]

The Court in *Riley* also dismissed proposals for limited searches or searches on additional grounds.[129] A limited or cursory search would entail "few meaningful constraints", because "the proposed categories would sweep in a great deal of information, and officers would not always be

[122] *Ibid.*

[123] *Ibid*, 2486.

[124] *Ibid*.

[125] *Ibid*, 2489.

[126] *Ibid*, 2479 and 2489.

[127] *Ibid*, 2491.

[128] *Ibid*: "Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."

[129] *Ibid*, 2491-93.

able to discern in advance what information would be found where."[130] The Court invoked its preference for "clear guidance to law enforcement through categorical rules"[131] to support a warrant requirement over a *Cotterman*-like rule allowing for limited searches on lesser grounds. Yet the Court also held that "even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone."[132] The question now is whether a border search is one such exception.

Border cases after Riley

A number of courts have since held that border device searches are indeed an exception to *Riley*.[133] But distinct approaches are emerging. The general trend is to hold that *Riley* does not apply to the border since the state interest in search in this context remains high. Yet in many of these cases, where the court touches on the question of state interest, it reverts to the pattern of reasoning prevalent in *Cotterman* and other pre-*Riley* cases of assuming the state's interest to be compelling without examining the issue, as the Court did in *Riley*.[134] Courts have tended to draw from *Riley* the narrow proposition that device searches engage a high privacy interest, but since even the most invasive border searches (including strip searches) are permissible on reasonable suspicion, only that standard should apply.[135] However, in a few instances, judges have taken up

[130] *Ibid*, 2492.

[131] *Ibid*, 2491, citing *Michigan v Summers*, 452 US 692, 705, n 19.

[132] *Riley*, *supra* note 5, 2494.

[133] *US v Saboonchi*, 48 F Supp 3d 815 (D Md 2014) [*Saboonchi 2*] 818; *United States v Molina-Isidoro*, 267 F Supp 3d 900 (WD Tex 2016) [*Molina 1*] 906; *United States v Vergara*, 884 F 3d 1309 (11th Cir 2018) [*Vergara*] 1313; and *United States v Touset*, 890 F 3d 1227 (11th Cir 2018) [*Touset*] 1234.

[134] In addition to *Saboonchi 2* and *Molina 1*, *ibid*, see also *United States v. Kolsuz*, 890 F 3d 133 (4th Cir. 2018) [*Kolsuz*]; *United States v Escarcega*, 685 Fed. App'x 354 (5th Cir 2017); *United States v Gonzales*, 6885 F App'x 867 (9th Cir 2016); and *United States v Mendez*, 240 F Supp 3d 1005 (D Ariz 2017); *United States v Caballero*, 178 F Supp 3d 1008 (SD Cal 2016) [*Caballaro*]; *United States v Ramos*, 190 F Supp 3d 992, 1002 (SD Cal 2016); *United States v Lopez*, No 13-CR-2092 WQH, 2016 WL 7370030 (SD Cal 2016); *United States v. Cano*, No 16-CR-01770-BTM, 2016 WL 6920449 (SD Cal 2016); and *United States v Hernandez*, No 15-CR-2613-GPC, 2016 WL 471943 (SD Cal 2016).

[135] In *Molina 1*, 907-8, the court concedes that a later appellate court might extend *Riley* to the border context, but that in the absence of authority holding that anything more than reasonable suspicion is required for a search at the border, it was compelled to find the device search in this case to be reasonable. The court in *Caballero*, *ibid*, was constrained to follow the 9th Circuit's decision in *Cotterman*, *supra* note 141, and held, 1018, which was not "clearly irreconcilable" with *Riley*. Applying similar reasoning, see also

Riley's invitation to probe the question of state of interest and have done so with greater skepticism.[136] Yet none of these opinions has formed part of a majority holding that requires a warrant for device searches at the border.

The decisions in *US v. Saboonchi*[137] and *US v Vergara*[138] are notable examples of the general trend to distinguish *Riley* without examining the question of state interest in any depth. *Saboonchi* involved the seizure of phones and a flash drive. Applying *Cotterman*, the District Court for Maryland dismissed a motion to suppress evidence obtained from the search, since it was conducted on reasonable suspicion.[139] The defendant brought a motion to reconsider in response to *Riley*. The court dismissed the motion on the basis that *Riley* "did not touch on the border search exception" and the reasoning in the original motion "largely accords with that of the Court" in *Riley*.[140]

The majority opinion in *Vergara*,[141] a decision of the Court of Appeals for the Eleventh Circuit, involved a motion to suppress evidence from a forensic search of two phones upon the accused's return from Mexico. The trial court had found that agents possessed reasonable suspicion for the search, a finding Vergara had not appealed. Counsel argued instead that in light

---

United States v Molina-Isidoro, 884 F 3d 287 (Fifth Cir 2018) [*Molina 2*]; *Kolsuz*, *ibid*; and *Vergara*, *supra* note 143.

[136] At the appellate level: Judge Costa's concurrence in *Molina 2*, *ibid*; *Vergara*, *supra* note 143; Wilkinson's concurrence in Kolsuz, *supra* note 144; and at trial: *United States v Kim*, 103 F Supp 3d 32 (DDC 2015) [*Kim*] and *Alasaad v Nielsen*, WL 2170323 (DDC 2018) [*Alasaad*] (discussed below).

[137] *Saboonchi* 2, *supra* note 133.

[138] *Vergara*, *supra* note 133.

[139] *United States v Saboonchi*, 990 F Supp 2d 536 (D Md 2014) [*Saboonchi 1*] at 571.

[140] *Saboonchi* 2, *supra* note 133, 816. Judge Grimm noted at 817 that *Riley* recognized that warrantless device searches might be reasonable in certain contexts, and held the border to be one such case. The "strength" of the state interest in "preventing the entry of unwanted persons and effects" rested on an "acknowledgement that a wide range of suspiciousless searches are 'reasonable simply by virtue of the fact that they occur at the border'" (citing *Flores-Montano*, *supra* note 99, 152). In Grimm J's view, at 819, "*Riley* did not diminish the Government's interests in protecting the border or the scope of the border search exception." His Honour was mistaken about the question *Riley* was raising here: not whether the state retained a pressing interest in search at the border, but in search of *data* at the border.

[141] *Supra* note 133.

of *Riley*, both manual and forensic phone searches require a warrant.[142] Writing for the majority, Judge William Pryor held that the Court in *Riley* "expressly limited its holding to the search-incident-to-arrest exception".[143] And since no earlier authority had found a standard higher than reasonable suspicion to be required for the most invasive border searches, despite *Riley*'s finding of a high privacy interest in digital devices, nothing more than reasonable suspicion could be required for data searches.[144]

However, some judges have taken up *Riley*'s invitation to explore the question of the state's interest in the search of data here in greater depth. At the trial level, two decisions to note are *US v Kim*[145] and *US v Alasaad*,[146] though neither resulted in a change in the standard for data searches.[147] *US v Molina-Isidoro*,[148] a case decided by the Court of Appeals for the Fifth Circuit, involved the search of the appellant's phone following the discovery of kilograms of meth in her suitcase. The appellant argued that the reasoning in *Riley* justified the requirement of a warrant on probable grounds for routine device searches.[149] The Court upheld the validity of the search on the basis that border agents had acted in reasonable reliance on existing law.[150] But in a

[142] *Ibid*, 1311.

[143] *Ibid*, 1312, citing *Riley*, *supra* note 5, 2494.

[144] *Vergara*, *supra* note 133, 1313. The remainder of the opinion assumes, without raising the issue, that the state retains a pressing interest in search at the border of both physical and digital spaces.

[145] *Kim*, *supra* note 136.

[146] *Alasaad*, *supra* note 136.

[147] *Kim*, *supra* note 136, involved the search of a laptop seized upon departure from the US. Judge Jackson granted the motion to suppress on the basis that the search was clearly not routine and lacked reasonable suspicion. Engaging with *Riley*'s analysis of state interest, her Honour assert at 56-57: "the immediate national security concerns [here] were somewhat attenuated" while "the invasion of privacy was substantial." In *Alasaad*, *supra* note 136, the court dismissed a motion to strike a challenge to the constitutionality of device searches at the border on the part of 11 travelers. Judge Casper relied on *Riley* in holding (at 40-41) that a plausible Fourth Amendment argument could be made on the basis of the high privacy interest in devices but also in light of the uncertainty as to the degree to which discoveries of contra-band through data searches are "prevalent".

[148] *Molina 2*, *supra* note 135.

[149] *Ibid*, 289.

[150] *Ibid*, 290, invoking the 'good faith' exception to the exclusionary rule: *United States v Curtis*, 635 F 3d 704, 713 (5th Cir. 2011) (citing *United States v Leon*, 468 US 897, 918, 104 S Ct 3405, 82 L Ed 2d 677 (1984).

concurring opinion, Costa J explored the question of whether, in light of *Riley*, device searches at the border should fall within the scope of the border search exception to the warrant requirement. His Honour cast doubt on the nexus between device searches and traditional border search purposes, noting that travelers tend not to conceal contraband in their devices.[151]

The dissenting opinion of Judge Jill Pryor in *Vergara*,[152] is close in spirit to Judge Costa's opinion. Judge Pryor disagreed with the majority in *Vergara* in its holding that *Riley* does not to apply to the border and that the state interest in data searches at the border remains pressing.[153] Asserting that *Riley*'s holdings about digital privacy apply at the border, her Honour reasoned that while the state might have a higher interest in search at the border than upon arrest, what would likely be turned up by a device search would advance general law enforcement rather than traditional border protection purposes.[154] In her view, the proper balance—with respect to *forensic* device searches at the border—requires a warrant on probable grounds.[155]

In summary, US law on border searches is similarly permissive as Canadian law of an approach to device searches as cursory and thus not requiring reasonable grounds or a warrant. As with Canadian courts, US courts are beginning to accept that devices retain a high privacy

---

[151] *Molina 2*, *supra* note 135, 296: "If contraband is not being electronically concealed in phones and computers, does the government still have as compelling an interest in searching those items at the border? The government argues it does because the interests in national security and fighting crime are especially weighty at the border and searches of technology can uncover evidence of border crimes. No doubt a text message or email may reveal evidence of crimes, but that is true both at and inside the border. But it is uncertain whether the evidence-gathering justification is so much stronger at the border that it supports warrantless and suspicionless searches of the phones of the millions crossing it." At 297 Judge Costa also distinguished between searches conducted for the purpose of "general crime fighting and national security", which device searches can advance, and searches conducted to discover contraband, which device searches cannot assist with. The question for the Supreme Court, Costa J speculated, is what weight to accord to the first of these purposes.

[152] *Vergara*, *supra* note 133.

[153] *Ibid*, 1313.

[154] *Ibid*, 1316-17: "To be sure, forensically searching a cell phone may lead to the discovery of physical contraband. A drug smuggler's deleted text messages, for example, may reveal the location of drugs inside the border. But this general law enforcement justification is quite far removed from the purpose originally underlying the border search exception: 'protecting this Nation from entrants who may bring anything harmful into this country'" (citing *Hernandez*, *supra* note 91, 544).

[155] *Vergara*, *supra* note 133, 1315.

interest—even at the border. Courts have also begun to question whether this calls for a higher standard for search. But in keeping with the pattern of Canadian courts, American judges have—with notable but few exceptions—been slow to call attention to the state interest in search or to assess it in much depth. The reluctance to do so runs contrary to the thrust of the Supreme Court's approach in *Riley*, but also to a body of scholarship that offers a valuable set of critical tools for assessing the issue.

Part II: Critical approaches to the state interest in border device searches

Scholarship on data search at the border is copious.[156] Yet, as noted, much of it focuses on the issue of privacy. As with most court decisions on point, the scholarship tends to assess the constitutionality of groundless border device searches primarily on the basis of the court's failure to accord sufficient weight to the privacy interest in devices—which commentators agree is high even at the border.[157] Much of the scholarship contends that device searches should require reasonable suspicion in all or most cases, but the consensus rests on the often-unquestioned assumption that the state retains a pressing interest not just in search but the search of data at the border.[158] Yet from as far back as 2008, a minority of scholars have been critical of the state's

[156] Recent literature includes Eunice Parks, 'The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post-*Riley*' (2017) 44:3 Hastings Const LQ 277; Jared Janes, 'The Border Search Doctrine in the Digital Age: Implications of Riley v. California on Border Law Enforcement's Authority for Warrantless Searches of Electronic Devices' (2016), 35 Rev Litig 71; Thomas Mann Miller, 'Digital Border Searches After Riley v. California' (2015) 90 Wash L Rev 1943; Michael Creta, 'A Step in the Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices During Border Searches in United States v. Cotterman' (2014) 55 BC L Rev E Supplement 31; Matthew B Kugler, 'The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study' (2014) 81 U Chi L Rev 1165; Tom Rechtin, 'Back to the Future of Your Laptop: How Backlash Over Prolonged Detention of Digital Devices in Border Searches Is Symptomatic of a Need for 'Reasonable Suspicion' in All Border Searches of Digital Devices' (2014) 7 The Crit: Critical Stud J 66; Samuel A Townsend, 'Laptop Searches at the Border and United States v. Cotterman' (2014) 94 BU L REV 1745.

[157] See, *eg*, Park, *ibid*.

[158] See, *eg*, Park, *ibid*, suggesting a "bright-line" rule for both routine and non-routine searches, with reasonable suspicion required for the latter; Andrew Pincus, "Evolving Technology and the Fourth Amendment: The Implications of *Riley v. California*, 2014 CATO Sup Ct Rev 307, querying, 336, whether *Riley*'s holding on the high privacy interest in devices will result in a future appellate decision requiring reasonable suspicion; and Ryne Spengler, "Hijacked at the Border: Why the Government Should Have

interest and have assessed reasonable border data search in this light.[159]

Critical approaches to the state's interest generally advance one or both of two distinct arguments. First, device searches bear no rational connection to the conventional purposes of search at the border or a tenuous one. Those purposes include preventing the unlawful entry of persons or physical goods over the border. Data can be considered a "good," and some unlawful data will enter the country carried on a device. But since the vast majority of unlawful data enters the country through the internet, the practice of groundless device searches at the border are a far less effective means of control of entry for this form of good.[160]

A second argument is closely related: given the small portion of unlawful data discovered

---

Reasonable Suspicion Before Conducting Intrusive Examinations of Our Personal Electronic Devices" (2015) 11 Seton Hal Cir Rev 431, arguing, at 452, that the analysis of device searches in *Riley* can be reconciled with the Ninth Circuit's decision in *Cotterman*, *supra* note 111, by requiring reasonable suspicion for all border device searches.

[159] Rasha Alzahabi, 'Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers' (2008) 41:1 Ind L Rev 161; Ari Fontecchio, 'Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception that Swallows Your Laptop' (2009) 31 Cardozo L Rev 231; Victoria Wilson, 'Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders From Bombs, Drugs, and the Pictures From Your Vacation' (2011) 65 U Miami L Rev 999; Janet Hoeffel and Stephen Singer, 'Fear and Loathing at the U.S. Border' (2013) 82:4 Miss LJ 1; Thomas Mann Miller, 'Digital Border Searches After Riley v. California' (2015) 90 Wash L Rev 1943. For Canadian scholarship, see Penney, *supra* note 8, and Robert Diab, *supra* note 8.

[160] Alzahabi, *ibid*, 177, noting that child pornography or other illicit files "will still enter into our country… due to the nature of the Internet and electronic communications"; Fontecchio, *ibid*, 235: since "data travels electronically via cyberspace" rather than over physical borders, "the government has no *special* need to search data at these physical borders separate and apart from searching data in computers already in the country"; Wilson, *ibid*, 1012-13, asserting that since there is "nothing exceptional or dangerous" about data carried in a device across the border, "the government's interest in searching data and information is lower"; Hoeffel and Singer, *ibid*, 13-4, observing that data "does not implicate the border" since it need not be "physically smuggled" into the country to be imported, as does other contraband and that cases on point to date "have almost all involved searches that uncovered images of child pornography", which is essentially a form of "ordinary crime control" rather than border control; Miller, *ibid*, 1992, questioning the tie between border data searches and conventional border search purposes, noting that while some information found on devices may pose a threat ("terrorist plans or certain classified information"), in other cases, including child porn, this is less clear; and Penny, *supra* note 8, 510-1, noting that the contraband at issue in most data search cases thus far is child pornography and "[e]ven if officials managed to intercept every incoming digital child pornography file at customs, it would do next to nothing to stem the availability (and concomitant harms) of child pornography in Canada."

through device searches—gleaned from the case law that deals mostly with child pornography—the invasiveness of routine searches outweighs the state's interest in the potential discovery of the evidence.[161] Put otherwise, even if the state carries out an important purpose in conducting device searches at the border, the meagre fruits of the practice of frequent and groundless searches suggests that they are an ineffective and disproportionate means of advancing those purposes.

These two common arguments against a pressing state interest support either a warrant standard or at the least a standard of reasonable grounds before a search can be conducted. A third argument can be offered in favour of a warrant standard in particular. The state has a less pressing interest in the search of data at the border than it does in search of the body. As noted in Part I, strip searches at the border in both Canada and the United States require reasonable suspicion.[162] Quite apart from the rate at which searches conducted pursuant to reasonable suspicion yield false positives—no evidence of contraband—in the cases that do result in the discovery of contraband, physical searches often play an indispensable role. They are, in many cases, the only means by which the state could have prevented the entry of the items. Given the vastly greater quantity of case law involving challenges to these searches, it is clear that discoveries of contraband in strip searches are far more frequent; therefore, the state's interest in carrying them out is far greater than it is in the case of illicit data.

An important counter-argument to all three claims in this Part should be acknowledged. All three of the arguments relate to the state's interest in preventing the entry of illicit *data* into the country. Both the Canada Border Services Agency and US Customs and Border Protection note a further purpose to conducting data searches: the discovery of evidence that may assist in detecting breaches of customs or immigration law that pertain to the unlawful entry of *persons or goods*.[163] Border officials might discover an email indicating that an expensive item in a traveler's possession was purchased through Craigslist and not declared for duty purposes. On this view,

[161] See *eg* Alzahabi, *supra*, note 159; Hoeffel and Singer, *supra*, note 159, 13-4; and Penny, *supra* note 8, 510-1.

[162] *Simmons*, *supra* note 24 and *Hernandez*, *supra* note 85.

[163] See the discussion of CBSA submissions to Parliament in Part III below; for the CBP, see *supra* note 104, 1.

the state's interest in conducting a search is pressing by virtue of being tied to the state's broader (pressing) interest in border law enforcement.

Searching phones to detect duty infringements may indeed be an important purpose. But the evidence from the case law, in both countries, does not support the view that this is a *pressing* state purpose. As noted in Part I, the vast majority of the cases dealing with border data searches in both jurisdictions relates to child pornography. Device searches may indeed be of some assistance to border officials in detecting border offences (relating to physical goods or immigration law), but if they were being used effectively in this way with any frequency, the case law would reflect it. While there may be the odd case in either jurisdiction, I am aware of only a single case and note that none is referred to in the scholarship on state interest surveyed above.[164]

In summary, over the past decade, in both Canada and the US, there has been a relatively small body of cases dealing with the fruit of device searches. The majority concern child pornography. The data at issue represents a tiny part of the cross-border traffic in such data, and therefore device searches for this purpose are not pressing. Nor do device searches appear to provide a significant form of assistance in detecting border offences of a physical nature. Thus, although the state has an interest in searching data at the border, the available evidence suggests it is limited and outweighed by the privacy interest at issue. Customs officials are carrying out groundless searches with some frequency, with questionable purpose, resulting in invasive and thus unreasonable searches. A more reasonable balance between state and individual interests here—a reasonable search—requires a warrant on probable grounds.

Part III: The question of the state's interest in debate about reform of device search powers

As noted at the outset of this paper, citizens in both Canada and the United States are becoming more concerned about the practice of groundless data searches at the border. Lawmakers in both countries have begun questioning whether such searches are reasonable. In ways to be explored,

[164] In *R v Bialski*, *supra* note 48, customs officials stop a couple entering Canada in a recreational vehicle they suspect may have been purchased in the US, contrary to the driver's declarations. Border officials search a laptop and two cellphones and discover evidence that it was purchased in the US.

recent reform efforts in Parliament and Congress point to a consensus that devices engage a high privacy interest. And lawmakers have begun to probe whether the state has a compelling interest in groundless or immediate access to device data at the border. Yet in both nations, lawmakers debate the question of state interest without clarity on the point. The aim of this part of the paper is to shed light on this shortcoming and to show how a clear case should be made, in future reform efforts, for border data search requiring a warrant.

Legislative reform efforts in Canada

In the summer and fall of 2017, the House of Commons Standing Committee on Access to Information, Privacy and Ethics held hearings to address "Canadians' privacy at airports and borders", including "the examination of digital devices at the border".[165] A range of groups and individuals made submissions to the Committee, including CBSA Vice President Martin Bolduc.[166] Both the transcript of the hearings[167] and the written submissions[168] indicate that—with one exception—there was no discussion of the state's purposes in the search of data at the border.

---

[165] Canada, House of Commons, Standing Committee on Access to Information, Privacy and Ethics: *Protecting Canadians' Privacy at the U.S. Border* (December 2017) (Chair: Bob Zimmer) ["Report"] at 3.

[166] See the appendix to the Report, *ibid*, 37.

[167] Meetings of the Standing Committee on Access to Information, Privacy Ethics, House of Commons, "Privacy of Canadians at Airports, Borders and Travelling in the United States" (Ottawa, 15 June; 18 and 27 September 2017) <https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=9566122> accessed 3 December 2018.

[168] Submissions include the Canadian Bar Association, 'Privacy of Canadians at Airports and Borders' (Toronto, September 2017) <http://www.cba.org/CMSPages/GetFile.aspx?guid=04e96564-b5b6-441b-b6de-20b3e0874975> accessed 3 December 2018; the Barreau du Québec 'Comments and Observations: Privacy and Personal Information Protection at Border Crossings and Airports' (Montreal, October 2017) <https://lawsdocbox.com/Legal_Issues/76628760-The-barreau-du-quebec-comments-and-observations.html> accessed 3 December 2018. But see also Michael Vonn and Meghan McDermott's submission for the British Columbia Civil Liberties Association, 'Presentation to the Standing Committee on Access to Information, Privacy and Ethics in its study of the Privacy of Canadians at Airports, Borders and Travelling in the United States' (Vancouver, 15 June 2017) <https://bccla.org/wp-content/uploads/2017/06/ETHI-presentation-Privacy-at-the-Border.pdf> accessed 3 December 2018; the Canadian Civil Liberties Association, 'Privacy at the Border: Committee Report Recommends Customs Act Update' (Toronto, 12 December 2017) <https://ccla.org/privacy-border-committee-report-recommends-customs-act-update/> accessed 3 December 2018; and Michael Geist, 'Appearance before the House of Commons Standing Committee on Access to Information, Privacy & Ethics' (Ottawa, September 27, 2017) <http://www.michaelgeist.ca/2017/10/border-airport-privacy-appearance-standing-committee-access-information-privacy-ethics/> accessed 3 December 2018.

Speakers were concerned almost exclusively with privacy.[169] The hearings dealt with matters in addition to device searches.[170] Yet the scope of CBSA device searches was a central issue.

The exception to the focus on privacy involved a line of questions raised by Committee members on the final day of evidence, in the course of Vice-President Martin Bolduc's submissions for the CBSA. Bolduc had asserted that searches are conducted only where there is a "clear link" with "CBSA-mandated program legislation", but that they were effective in enforcement of that mandate, since they "may uncover a range of customs-related offences.[171] In addition to child pornography, devices searches could uncover "electronic receipts [that] may prove that goods have been deliberately undervalued or undeclared."[172] On behalf of the Committee, Member of Parliament Jacques Gourde asked whether Bolduc believed "the number of electronic device searches you have conducted has really been worthwhile? Has something come up one time out of 1,000? Is it really worth continuing the exercise?"[173] Bolduc replied:

> If the agency believed that such examinations were not worthwhile, we would stop doing them. Unfortunately, we find child pornography and propaganda material on phones. In addition, in the case of people who said that they have not acquired anything on their trips, we find receipts on their phones that show otherwise. That examination is valid.

Yet, when asked to be more specific, Bolduc indicated the CBSA had not tracked the number and nature of searches—but had begun to do so weeks earlier and would make this public in due

---

[169] The CBA's argument as to the constitutional invalidity of groundless searches is focused exclusively on the extent of the privacy invasion entailed in device searches. Its issue with earlier cases is also confined to privacy; at 9, *ibid*: "A number of cases on electronic device searches at border crossings have improperly focused on the quantity of information these devices possess in drawing comparisons with other storage containers like briefcases or luggage. It is equally important to consider that these devices contain a wide variety of *types* of information in any analysis." The Barreau de Québec brief, *ibid*, is concerned mostly with the searches affecting the solicitor-client relationship and contains no discussion of state purposes in the search of data. Neither the BCCLA nor Geist's submission, nor the CCLA's summary of its submission noted, *ibid*, address the state interest in data searches.

[170] See Report, *supra* note 165, at 3, for a list of issues the Committee sought to explore (the 'preclearance' bill allowing for search by US officials on Canadian soil and information sharing of data obtained by CBSA, among others).

[171] Meeting of September 27, 2017, *supra* note 167 at 15:40 of the transcript.

[172] *ibid*.

[173] *Ibid*, at 15:50.

course.[174]

The Committee was clearly interested in whether border data searches bear a rational connection to the state's objectives in search at the border, and whether they advance them effectively. Bolduc offered evidence of *a* connection—in addition to child porn, or other illicit files, data searches can uncover failures to declare physical goods or false declarations. But without knowing how often this happens in relation to the number of device searches carried out, the Committee could not discern whether the connection Bolduc asserted here was more than theoretical or speculative—as the dissent in *Fearon* had held to be the case with device searches on arrest.

One point that might have been made in response to Bolduc is that the available evidence does not support his claim. As noted in Part II above, if data searches have been effective in discovering that people are undervaluing the goods they declare, or failing to declare them, there would likely be a body of cases in which at least a few such searches have been challenged.[175] As noted, among the eleven Canadian decisions on border devices searches, eight involve child pornography, and only one case involves a device search that reveals evidence of a false declaration.[176] One reported decision in over a decade of device searches undermines the claim that such searches are frequently effective in enforcing duties and thus pressing.

However, the Committee chose not to wait for further statistics on search before tabling its final report in December of 2017. The report entirely omits the question of the state's purposes in searching data at the border, and focuses almost exclusively on privacy.[177] Groups aside from

---

[174] *Ibid*, see the exchange between Jacques Gourde and Martin Bolduc, 15:45. See also Mathew Braga, "Canada's Border Agency to Start Tracking", *supra* note 36.

[175] A search carried out on suspicion of a failure to report or a false declaration, contrary to sections 12 and 13 of the Act, *supra* note 22, would be carried out pursuant to 98(1) and of goods under section 99(1)(c.1) to (f), noted above—thus falling within the class of cases canvassed earlier.

[176] The false declaration case is *Bialski*, *supra* note 48 and discussed *supra* note 164. Eight of the eleven cases are referred to *supra* note 37 (*Leask*, *Mozo*, *Whittaker*, *Saikaley*, *Moroz*, *Buss*, *Gibson*, and *Canfield*), leaving *Bares*, *Appleton*, and *Bialski* cited *supra* note 48. All aside from *Saikaley*, *Appleton*, and *Bialski* involve child pornography. In *Saikaley*, officials, acting on information provided by the RCMP, discover a drug-debt list. *Appleton* involves a text message. In this case, customs officers discover a gun in the glove box of a vehicle, learn from US officials that it was stolen, and then proceed to search the phone.

[177] The Committee acknowledges the thrust of recent Supreme Court jurisprudence on the high privacy

the CBSA generally agreed that reasonable suspicion was an appropriate standard.[178] Among the Committee's recommendations were that CBSA's 2015 Guidelines "be written into the *Customs Act*"[179] and that the standard of a "multiplicity of indicators" be replaced with "reasonable grounds to suspect."[180] The report urges government to track the number of device searches and to provide regular updates to the Privacy Commissioner of Canada.[181] The Committee had thus done what the majority in *Fearon* had done: assumed that a *possible* state interest in the search of device data justifies a warrantless search, despite recognizing the high degree of privacy in device data.

In April of 2018, Public Safety Minister Ralph Goodale responded to the Committee's December report.[182] He shared the view that device searches should be tracked but declined to accept the recommendation that the *Customs Act* be amended to codify a particular standard. In the government's view, the CBSA's policy of not carrying out searches routinely and requiring a "multiplicity of indicators" suffices for the present. He believed the policy to be justified in light of the fact that device searches *could* help "discover customs-related contraventions" including undervalued or undeclared goods.[183] Anything more formal (statutory codification of the standard) would unnecessarily hinder the CBSA's "ability to respond to emerging threats and contraventions" of border law.[184] Here too, the government's response mirrors the majority's approach in *Fearon*: the state's pressing interest in immediate access to data rests on the *possibility*

---

interest in devices, and expresses a laudable concern about the "lack of clear rules" in the *Customs Act*: Report, *supra* note 165, 5.

[178] *Ibid* at 9 and 10. Brenda McPhail, for the Canadian Civil Liberties Association, is cited as suggesting a warrant requirement at 10.

[179] The Report, *supra* note 165, 11.

[180] *Ibid*, 1. Among the other recommendations was a call upon the government to track the number of device searches at the border and provide the information to the Privacy Commissioner of Canada (at 13). Another, at 2, was that "the Government of Canada consider establishing internal privacy and civil liberties officers within the Canada Border Services Agency to monitor privacy issues at the agency level".

[181] *Ibid*, 13.

[182] Minister of Public Safety and Emergency Preparedness, Ralph Goodale, letter of 16 April 2018 to Bob Zimmer, Chair of the House of Commons Standing Committee on Access to Information, Privacy and Ethics, online: <http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-10/response-8512-421-330>.

[183] *Ibid.*

[184] *Ibid.*

that data searches will assist with "emerging threats".

The CBSA may soon report on the number of device searches and the nature of the evidence they uncover. This may provide evidence that device searches help to uncover unpaid duties or false declarations with some frequency. But the case law suggests that the annual number of those discoveries is not likely to be high in relation to the number of searches the CBSA conducts. The numbers are likely to show that most searches resulting in offences relate to child pornography. If the numbers are consistent with these predictions, the only reasonable inference to draw from the CBSA's practice of border device searches is that the state's interest in immediate, warrantless data search is not pressing or compelling.

Ideally, courts in the near future will have statistical evidence of CBSA search practices to draw upon when assessing whether groundless border data searches are reasonable under section 8 of the *Charter*. Courts should also draw upon the dissent's approach in *Fearon* as a model for assessing state interest in device searches. A court that more closely examines state interest in the border context – in light of the evidence – should conclude (as did the dissent in *Fearon* in the context of arrest) that border data searches bear only a tenuous connection to border search purposes, and a practical effectiveness that is remote or speculative. Assuming the high privacy interest in device data, a reasonable search power of data at the border should require a warrant.

Legislative reform efforts in the US

In April of 2017 a bi-partisan bill, titled the *Protecting Data at the Border Act* (PDBA), was introduced in Congress.[185] The bill would require officials to obtain a warrant on probable grounds before searching device data at the border—although the bill's protections apply only to US citizens. The bill would also prohibit denying entry for refusal to provide a password or unlock a device; it would require officers to notify travelers of the right to refuse requests to provide access and require probable grounds for confiscating a device; and it would prohibit the

[185] *Protecting Data at the Border Act*, S 823, HR 1899, 115th Congress; introduced in April 2017 by Senators Ron Wyden (D-Ore.), and Rand Paul (R-Ky.); and Representatives Jared Polis (D-Colo.), Blake Farenthold (R-Texas), and Adam Smith (D-Wash). For further details, see Adam Schwartz and Sophia Cope, "Pass the Protecting Data at the Border Act" *The Hill* (28 September 2017).

admission of evidence obtained in violation of the bill.[186]

The PDBA may never be passed and has since been followed by the tabling of another bill proposing a reasonable suspicion standard.[187] But debate on the PDBA suggests a measure of political consensus on the view that a reasonable border data search requires a warrant. Yet, here too, critical opinion on the state's interest in search might have played a more prominent role.

The preamble of the PDBA cites *Riley* for the proposition that devices engage a high degree of privacy.[188] Senator Wyden, one of the bill's sponsors, indicated in a press release that the bill "recognizes the principles from [*Riley*] extend to searches of digital devices at the border." [189] He thus implied here that a higher standard for device searches at the border rests on both the higher privacy interest and the less compelling state interest in immediate access to data (less compelling than in physical searches in some cases). But without making explicit how the bill draws on *Riley* for support, the argument in favour of a warrant standard appears to rest mainly on privacy. This is how much of the supportive coverage of the bill has been framed, among media and groups such as the Electronic Frontier Foundation, Techcrunch, and The Verge.[190]

In the limited public debate on the bill's merits, the question of the state interest in data searches has been more prominent. Counsel for Homeland Security arguing in favour of the status quo on device searches asserted in an op-ed in *USA Today* that "electronic media searches have produced information used to combat terrorism, violations of export controls, and

---

[186] Schwartz and Cope, *ibid*.

[187] *A bill to place restrictions on searches and seizures of electronic devices at the border*, S 2463, 115th Congress; introduced February 27, 2018 by Senator Leahy (D-VT); read twice and currently referred to the Committee on Homeland Security and Governmental Affairs.

[188] *Supra*, note 185.

[189] See "Wyden, Paul, Polis and Farenthold Bill Requires Warrants to Search Americans' Digital Devices at the Border" (4 April 2017) online: wyden.senate.gov.

[190] See *eg*, Adam Schwartz and Sophia Cope 'Pass the Protecting Data at the Border Act' EFF.org (San Francisco, 13 October 2017) <https://www.eff.org/deeplinks/2017/10/pass-protecting-data-border-act> accessed 3 December 2018; Taylor Hatmaker, 'New Bipartisan Bill Seeks to Stop Warrantless Device Searches at US Borders' techrunch.com (San Francisco, 4 April 2017) <https://techcrunch.com/2017/04/04/protecting-data-at-the-border-act-wyden/> accessed 3 December 2018; Adi Robertson, 'New Bill Would Crack Down on Border Phone Searches Without Warrants' verge.com (New York, 4 April 2017) <https://www.theverge.com/2017/4/4/15180244/protecting-data-border-act-wyden-paul-device-security-bill> accessed 3 December 2018.

convictions for child pornography, intellectual property rights violations and visa fraud."[191] They are thus "critical to our mission". Yet he provided no particulars. He invoked no high-profile cases of a terror plot foiled, or statistics on the rate at which groundless searches yield evidence of serious border offences. Consistent with the pattern of government argument in the case law and post-*Riley* litigation, assertions about the importance of unhindered access to devices were to be taken on faith. By contrast, opinion in support of the bill has sought to challenge these claims.[192] One commentator noted the limited purposes of the border search exception—preventing illicit entry of people and goods—and questioned how the importing of data conforms to these purposes.[193] Where combating terrorism, IP violations, or child pornography are invoked as grounds for search authority, border officials are no longer primarily policing the border but carrying on "investigatory work … on behalf of other enforcement agencies".[194]

Thus, in the course of debate on law reform of device searches in both Canada and the US, some skepticism has been expressed about whether the state has a pressing interest in immediate, groundless access to device data. But the voices have been few in number and the arguments have not played a prominent role in reform advocacy and debate. However, where they are made and made clearly, the assessments of what constitutes a reasonable search in this context are better informed. And in the absence of evidence that groundless devices searches are effective means of advancing conventional border search purposes, the argument against a compelling state interest in data search supports a higher standard for device searches.

Conclusion

In both Canada and the United States, courts, state agencies, and law scholars have now grappled with the issue of digital privacy at the border for over a decade. Courts are only now beginning to

[191] Joseph Maher, 'DHS: Device Searches Improve Safety' *USA Today* (McLean Virginia, 27 March 2017).

[192] Nicole Kardell, 'You Have a Right to Your Data at the Border' Foundation for Economic Education (18 November 2017) <https://fee.org/articles/you-have-a-right-to-your-data-at-the-border/> accessed 3 December 2018; Brian Feldman, 'A Former NSA Lawyer Explains Why Searching Phones at the Border Is a Waste of Time' yahoo.com (21 April 2017) <https://finance.yahoo.com/news/former-nsa-lawyer-explains-why-192603591.html> accessed 3 December 2018.

[193] Kardell, *ibid*.

[194] *Ibid*.

accept the high privacy interest in devices and their essential difference from physical containers. But they have been slow to recognize a distinction between the state's interest in search at the border and its interest in the search of data at the border. Failing to do so, courts have been quick to assume that digital searches may engage significant privacy interests but do not fundamentally alter the assessment of reasonable search at the border. The US Supreme Court's analysis in *Riley* and the dissent's analysis in the Supreme Court of Canada's decision in *Fearon* demonstrate that a careful assessment of state purposes in device searches in the context at issue leads to different conclusions about reasonableness.

In ways made clear in *Riley* and *Fearon*, and in a body a scholarship critical of the state's interest in data search at the border, a more rigorous assessment of what is reasonable in this context depends on a closer examination of whether data searches bear a rational connection to the state's purposes in search at the border, and how effective they are in practice at advancing these purposes. Both questions have begun to play a more prominent role in litigation, but they played only a limited in role in recent law reform efforts.

This paper has gathered together the range of arguments against the claim that the state has a pressing interest in device searches, and to demonstrate why these arguments should be play a more prominent role in court challenges and law-reform debate. Before courts or lawmakers come to conclusions about what constitutes reasonable search in the case of device searches at the border, they should assess not only the privacy interest at issue but also the state's interest in carrying out the search. In the absence of clear evidence that routine searches substantially advance the state's interest in preventing border and immigration offences, device searches at the border should not be exempt from the normal requirement of a warrant.