PROTECTING THE RIGHT TO PRIVACY IN DIGITAL DEVICES: REASONABLE SEARCH ON ARREST AND AT THE BORDER

Robert Diab*

Abstract

Canada's courts in recent years have consistently recognized a high degree of privacy in the content of digital devices. Yet the law authorizing device searches on arrest and at the border has failed to reflect this higher interest. In both contexts, courts have assumed that the state has a compelling interest in immediate access to device data to advance pressing law enforcement objectives – but the claim is not supported by evidence. This paper builds upon earlier critical views of device search law and policy by demonstrating that searches are being carried out on arrest and at the border without clear limits, resulting in significant intrusions into personal privacy, and without effective avenues of recourse.

Part I critically examines the Supreme Court's justification in *Fearon* for authorizing device searches on arrest, including its dismissal of the US Supreme Court's approach in *Riley v California* (requiring a warrant). It then presents evidence to support the dissent's argument that the majority's test provides ineffective guidance to police to avoid unreasonable searches, and that the exclusion of evidence is not an adequate remedy. Part II examines the Canada Border Services Agency's rationale and practice for groundless device searches under the *Customs Act*. It considers proposals for reform, including a Parliamentary report in late 2017 recommending a requirement of reasonable suspicion. Finally, it argues that the guarantee against unreasonable search in section 8 of the *Charter* requires a warrant for device searches at the border, because the state's interest in searching devices there is less pressing than the state's interest in searching a person.

Introduction

Canadians place a high value on their digital privacy and are concerned about its protection.[1] The Supreme Court of Canada, in a series of decisions from *Morelli*[2] to

* Robert Diab, LLB, LLM, PhD is an Associate Professor in the Faculty of Law at Thompson Rivers University (rdiab@tru.ca). He would like to thank Michael Vonn and Chris Hunt; the anonymous reviewers of this article; and Meg Collins and her co-editors at the UNB Law Journal.

[1] Public Safety Canada, *National Security Consultations: What We Learned* (Ottawa: Hill + Knowlton Strategies, May 2017) at 4.

[2] *R v Morelli*, 2010 SCC 8, [2010] 1 SCR 253 [*Morelli*].

Marakah,[3] has agreed. As Justice Fish 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."[4] Writing for the dissent in *R v Fearon*,[5] Justice Karakatsanis held that

> [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.[6]

The Court's computer cases contain many similar passages.[7] The higher privacy interest in personal data generally calls for a higher standard when assessing what constitutes a reasonable search under section 8 of the *Charter*.[8]

Two areas where an appropriate standard is lacking are search incident to arrest and search at the border.[9] The government has sought to defend the state's immediate need to access device data on arrest and at the border to advance pressing law enforcement objectives – but the claim is not supported by evidence and is contrary to common sense. This paper builds upon earlier critical views of device search law and policy (canvased below) by demonstrating that searches are being carried out on arrest and at the border without clear limits, resulting in significant intrusions into personal privacy, and without effective avenues of recourse.

Part I of this paper revisits the Supreme Court of Canada's decision in *R v Fearon*,[10] which allows police to search a device incident to arrest without a warrant. It argues that the majority failed to set out a sufficiently clear and effective rule to guide police to avoid unreasonable searches before they occur. It also argues that the majority's dismissal of the approach of the United States Supreme Court in *Riley v*

---

[3] *R v Marakah*, 2017 SCC 59, [2017] 2 SCR 608 [*Marakah*].

[4] *Morelli*, *supra* note 2 at para 2.

[5] *Fearon*, 2014 SCC 77, [2014] 3 SCR 621 [*Fearon*].

[6] *Ibid* at para 152.

[7] The most extensive discussion is set out in *R v Vu*, 2013 SCC 60, [2013] 3 SCR 657 [*Vu*], discussed below; see also *Morelli*, *supra* note 2 at paras 1 and 105–106; *R v Cole*, 2012 SCC 34 at paras 47–49, [2012] 3 SCR 34 [*Cole*]; and *R v Spencer*, 2014 SCC 43 at para 50, [2014] 2 SCR 212 [*Spencer*].

[8] *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*]. See *Vu*, *supra* note 7 on the need for a separate search warrant for computers in the course of a warranted search; *Fearon*, *supra* note 5 for search on arrest; *Spencer*, *supra* note 7 requiring a warrant for police searches of basic subscriber information held by an internet service provider.

[9] A further context is in relation to lawful access; see Matthew Ponsford, "The Lawful Access Fallacy: Voluntary Warrantless Disclosures, Customer Privacy, and Government Requests for Subscriber Information" (2017) 15 CJLT 153.

[10] *Fearon*, *supra* note 5.

California[11] (requiring a warrant) was premised on speculative and unsubstantiated assumptions about the threat posed by device data and the value of immediate access to it. Case law is cited in support of the dissent's concerns about the "overly complicated"[12] nature of the majority's rule, and the potential for serious privacy invasions where the rule is misapplied. This part concludes by considering the dissent's view that the exclusion of evidence would not be an adequate remedy for a serious breach in this context. A brief survey of remedies, or avenues of redress, including *Charter* and tort damages, and complaints to police or privacy oversight bodies, supports this view.

Part II of the paper examines the constitutional validity of device searches at the border, which are presently carried out without a warrant and without grounds. It looks first at law under which groundless searches at the border have been held reasonable under section 8 of the *Charter*. It then considers provisions of the *Customs Act*[13] on which the Canada Border Services Agency claims authority to carry out device searches without grounds, and proposals for reform, including a report tabled in late 2017 by a Parliamentary committee recommending the standard of reasonable suspicion.[14] The paper concludes by arguing that a reasonable search under section 8 in this context requires a warrant, except in exigent circumstances, on the basis of a lower state interest in the search of a device at the border than in the search of a person.

Part I: Search of devices upon arrest

Police have long possessed the authority to carry out a search incident to arrest.[15] Whether and if this should extend to the search of devices on arrest draws on two earlier threads in the Supreme Court's jurisprudence: the privacy interest in computers and the test for assessing whether a search power is reasonable in relation to the *Charter*. I look briefly at these two points before proceeding to *Fearon.*

In *Hunter v Southam*,[16] the Supreme Court held that the purpose of the guarantee against "unreasonable search" in section 8 of the *Charter* is to protect a person's reasonable expectation of privacy.[17] A reasonable search is one in which a person's privacy interest is reasonably outweighed by the state's interest in law

[11] *Riley v California*, 134 S Ct 2473 (2014), 189 L Ed (2d) 430 [*Riley*] (citations to the 'slip opinion').

[12] *Fearon*, *supra* note 5 at para 105.

[13] *Customs Act*, RSC 1985, c 1 (2nd Supp) [*Customs Act*].

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

[15] *Cloutier v Langlois*, [1990] 1 SCR 158, [1990] SCJ No 10 [*Cloutier*].

[16] *Hunter v Southam Inc*, [1984] 2 SCR 145, 11 DLR (4th) 641 [*Hunter*].

[17] *Ibid* at 159.

enforcement.[18] In the ordinary course, this occurs where police obtain a warrant issued on probable grounds.[19] A warrantless search would be *prima facie* unreasonable, the Court in *Hunter* held, but the Crown could rebut the presumption.[20] The Court recognized that in some situations either the individual or state interest might be higher or lower, calling for a different standard than a warrant on probable grounds.[21] The Supreme Court in *Collins* broadened this analysis by holding that a search will be reasonable under section 8 if it is authorized by law, if the law itself is reasonable, and if the search is carried out in a reasonable manner.[22] The question in the case of a new search power is whether the law that authorizes it is reasonable under the balancing of interests noted in *Hunter*.

In *Cloutier v Langlois*,[23] the Supreme Court recognized the validity of an ancillary police power upon arrest to carry out a brief pat down search or a search of a person's possessions or immediate surroundings without a warrant or additional grounds.[24] The power is confined within limits. A search on arrest must be connected to a criminal justice purpose related to the reason for the arrest, including safety, preventing escape, or gathering evidence.[25] The power does not authorize police to search spaces beyond the immediate vicinity of the arrest[26] or to take bodily samples.[27] The Court in *Golden* held that given the inherently invasive nature of strip searches, police need additional reasonable grounds to carry them out upon arrest.[28]

As cellphones became pervasive, courts grappled with whether search incident to arrest could extend to digital devices. Courts had been divided on the issue, due in part to a disagreement as to whether phones or computers are comparable to briefcases

---

[18] *Ibid* at 160.

[19] *Ibid* at 160, 167.

[20] *Ibid* at 161.

[21] *Ibid* at 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."

[22] *R v Collins*, [1987] 1 SCR 265 at 278, 38 DLR (4th) 508.

[23] *Cloutier*, *supra* note 15.

[24] *Ibid* at 182, referring to the balance of interests; see also *R v Stillman*, [1997] 1 SCR 607 at para 27, 144 DLR (4th) 193 [*Stillman*]; *R v Caslake*, [1998] 1 SCR 51 at paras 12, 14, 155 DLR (4th) 19 [*Caslake*]; *R v Golden*, 2001 SCC 83 at paras 44, 49, 75 and 104, [2001] 3 SCR 679 [*Golden*]; *R v Nolet*, 2010 SCC 24 at paras 49 and 52, [2010] 1 SCR 851; and *Fearon*, *supra* note 5 at para 45.

[25] *Cloutier*, *supra* note 15 at 186.

[26] *Ibid* at 180; *Caslake*, *supra* note 24 at para 40.

[27] *Stillman*, *supra* note 24 at para 89.

[28] *Golden*, *supra* note 24 at paras 98–99.

or other physical receptacles.[29] By the time *Fearon* had reached the Supreme Court, the Court had settled this more fundamental question in *R v Vu.*[30]

Vu dealt with the issue of whether a warrant to search a place in which a computer was found allowed police to search data on the computer. Justice Cromwell, writing for a unanimous Court, held that a separate warrant is required because "[t]he privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets."[31] In arriving at this conclusion, Justice Cromwell declined to accept a series of propositions that would become central to the majority's reasoning in *Fearon*. The Crown had argued that after-the-fact review of the reasonableness of a computer search was adequate protection of privacy in these cases.[32] The Crown also asserted that "computer searches are not all alike and different principles of search and seizure may be engaged depending on the circumstances in which the authorities encounter a computer."[33] It also contended that "requiring specific authority to search computers would restrict access to valuable information and undermine legitimate investigations."[34] Justice Cromwell dismissed all three arguments in light of the emphasis he placed on the privacy interests at stake in a computer.

The *Vu* decision featured an extended section – a short essay – on why computers are special and distinct, marking the culmination of such pronouncements from *Morelli* onward.[35] Beginning with the assertion that "[i]t is difficult to imagine a more intrusive invasion of privacy than the search of a personal or home computer,"[36] Justice Cromwell set out four distinguishing characteristics. Computers store "immense amounts of information" of an incomparable "scale and variety", engaging the "biographical core of personal information" referred to in *R v Plant*.[37] Computers

---

[29] See, e.g., *R v Polius* (2009), 196 CRR (2d) 288, 2009 CarswellOnt 4213 (Ont SC) holding that devices are not like briefcases and *R v Giles*, 2007 BCSC 1147 at para 63, 77 WCB (2d) 469 per MacKenzie J holding that: "… the information contained in the BlackBerry […] is not different in nature from what might be disclosed by searching a notebook, a briefcase or a purse found in the same circumstances." See also *R v Leask*, 2008 ONCJ 25 at para 16, 167 CRR (2d) 267 per 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 smartphone.

[30] *Vu*, *supra* note 7.

[31] *Ibid* at para 24.

[32] *Ibid* at paras 20, 34.

[33] *Ibid* at para 36.

[34] *Ibid*.

[35] The passage in *Vu*, *supra* note 7, appears at paras 40–45, drawing on earlier holdings in *Morelli*, *supra* note 2 at paras 1, 105–106; *Cole*, *supra* note 7 at paras 47–49.

[36] *Vu*, *supra* note 7 at para 45, citing *Morelli*, *supra* note 2 at para 105 per Fish J.

[37] *R v Plant*, [1993] 3 SCR 281 at 293, 24 CR (4th) 47. Cited in *Vu*, *supra* note 7 at para 41.

contain information "automatically generated, often unbeknownst to the user."[38] A computer also "retains files and data even after users think that they have destroyed them."[39] Finally, the search carried out in one place is not "a meaningful limitation with respect to computer searches."[40] Unlike documents found in a filing cabinet, information accessible on a computer can be located elsewhere. As a consequence of these "numerous and striking differences" between computers and physical receptacles, Justice Cromwell held that computers "call for distinctive treatment under s. 8 of the *Charter*."[41]

The following year, the Supreme Court turned to the issue of whether and when a device search incident to arrest may be reasonable in *R v Fearon*.[42] The accused in this case was arrested for the armed robbery of a jeweler in Toronto in 2009. Police found a cellphone in Fearon's pocket in the course of a pat-down search. The phone was unlocked and the officer viewed a number of text messages and photos, including the photo of a gun.[43] The phone was examined again later that evening by a second officer who found an unsent text message stating "We did it were the jewlery at nigga burrrrrrrrrr" [sic].[44]

The Court's holdings from *Morelli* to *Vu* had given rise to the expectation that a phone search on arrest would require a warrant.[45] Yet the Court was divided on the question 4 to 3. Justice Cromwell, writing for the majority (McLachlin CJ, along with Moldaver and Wagner JJ), held that a search incident to arrest could extend to a digital device – without a warrant – under certain conditions. The majority had unsettled expectations in *Fearon* due in large part to a shift in perspective on the state's interest in this context.

---

[38] *Vu, supra* note 7 at para 42.

[39] *Ibid* at para 43.

[40] *Ibid* at para 44.

[41] *Ibid* at para 45.

[42] *Fearon, supra* note 5.

[43] In a case comment on *Fearon,* Jordan Fine notes the limited capacity of the phone seized in this case, raising the possibility that the majority's perception of the potential impact of the rule at issue was affected in part by the limitations of the particular device in this case and the limited data it yielded when Fearon was searched: "Fearon's phone is described in the trial court judgment as a Telus LG285, a discontinued flip phone within the 'burner' class of devices, lacking a touchscreen, high-resolution camera, and social media application capabilities. To suggest that this phone bears any similarity to an iPhone 6 is akin to comparing a MacBook Air to a Commodore 64." Jordan Fine, "Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smartphone Data Granted in *R v Fearon*" (2015) 13 CJLT 171 at 179. See also Colton Fehr & Jared Biden, "Divorced From (Technological) Reality: A Response to the Supreme Court of Canada's Reasons in *R. v. Fearon*" (2015) 20:1 Can Crim L Rev 93 at 100, that "identity protection functions" such as touch and face-ID, "raise additional constitutional concerns about the rights to silence and against self-incrimination, as well as provide additional privacy interests that were not given weight by either the majority or the dissent in *Fearon*."

[44] *Fearon, supra* note 5 at para 107.

[45] Steven Penney, "Searches of Digital Devices Incident to Arrest: *R v Fearon*" (2014) 23:2 Const Forum Const 1 at 2.

The shift was premised on three propositions. First, law enforcement agents have a compelling interest in immediate access to cell phones on arrest due to the potential misuse of a device to "evade or resist" police, "call for 'backup'," or signal others to escape or destroy evidence.[46] Device searches are thus unlike the taking of bodily samples considered in *Stillman*,[47] since there is no urgency to those searches, whereas the search of data on arrest may in some cases be pressing.[48] But notably, Justice Cromwell spoke throughout this part of his analysis in a hypothetical tenor: "[p]rompt access" to data "*may* serve the purpose of identifying accomplices," etc.[49] Aside from passing mention to a single case – a US decision from 2008 (pre-dating smart phones) – Justice Cromwell cited no statistics or other evidence as to the frequency or usefulness of data gleaned from searches on arrest, and no cases to demonstrate that his assertions about state urgency here were more than hypothetical. He also omitted to address Chief Justice Roberts' significant discussion and dismissal of this argument (explored further below) in the analogous United States Supreme Court decision from earlier that year in *Riley v California*.[50]

The second premise was that although some device searches "may constitute very significant intrusions of privacy," as Justice Cromwell noted, "not every search is inevitably a significant intrusion."[51] This entailed a clear break from the thrust of *Vu*, where the focus was on the *capacity* of computers as such. By contrast, the limited search in this case, involving a text message and the photo of a handgun, was held to be "minimal," and formed the basis for distinguishing between minor and more invasive computer searches.[52] For the majority:

> a cell phone search is completely different from the seizure of bodily samples in *Stillman* and the strip search in *Golden*. Such searches are invariably and inherently very great invasions of privacy and are, in addition, a significant affront to human dignity. That cannot be said of cell phone searches incident to arrest.[53]

His earlier opinion in *Vu* on the distinctness of computers – the theory of its four capacities – now only merited a brief and passing mention.[54]

---

[46] *Fearon, supra* note 5 at para 48.

[47] *Stillman, supra* note 24.

[48] *Ibid* at paras 49 and 59.

[49] *Fearon, supra* note 5 at para 48.

[50] *Riley, supra* note 11.

[51] *Fearon, supra* note 5 at para 54.

[52] *Ibid.*

[53] *Ibid* at para 55; *Stillman* and *Golden, supra* note 24.

[54] *Ibid* at para 51. Justice Cromwell also reframed his characterization of the nature of computers here by speaking of their special capacities in the conditional tense: at para 51 of *Fearon, supra* note 5, computers "*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

A third key consideration was that "a person who has been lawfully arrested has a lower reasonable expectation of privacy than persons not under lawful arrest".[55] The heightened privacy interest in digital devices did not change the calculus here. Nor did Justice Cromwell seek to reconcile the notion of an arrestee's lower expectation of privacy with the point he noted earlier in the opinion (and in *Vu*) about device searches providing "access to information that is in no meaningful sense 'at' the location of the search".[56]

By extending the power of search incident to arrest to include digital devices, the Supreme Court declined to follow the approach of the US Supreme Court in *Riley*.[57] Before considering Justice Cromwell's justification for this, a brief consideration of *Riley* lends useful context.

The US Supreme Court in *Riley* held that the balance of state and individual interests does not favour warrantless searches because the search of a phone on arrest did not advance the state interests of officer safety and preservation of evidence that justify warrantless searches incident to arrest.[58] The finding here was premised on the holding that digital data "implicates substantially greater individual privacy interests than a brief physical search" and that data on a phone "cannot itself be used as a weapon to harm an arresting officer or to effectuate an arrestee's escape."[59] Concerns about the use of phone data as a means of warning officers about potentially threatening conduct of other parties was a concern "better addressed through consideration of case-specific exceptions to the warrant requirement, such as exigent circumstances."[60] The Court also favoured the warrant requirement here as consistent with its "general preference to provide clear guidance to law enforcement through categorical rules."[61]

Justice Cromwell did not engage with the US Supreme Court's contrary analysis of the potential danger digital data may pose on arrest. As Tim Quigley has noted, Justice Cromwell failed to explain why the concerns he raised about potential misuses of a device could not be addressed by the exigent circumstances exception, as

---

thinks that it has been destroyed, and *may* provide access to information that is in no meaningful sense 'at' the location of the search" [emphasis added].

[55] *Fearon*, *supra* note 5 at para 56, citing *R v Beare*, [1988] 2 SCR 387 at 413, 55 DLR (4th) 481.

[56] *Ibid* at para 51; and *Vu*, *supra* note 7 at para 44. Justice Cromwell's point here also runs contrary to the Court's recent approach in *Marakah*, *supra* note 3 (a case dealing with privacy in text messages) to de-emphasize *where* a search takes place in favour of an emphasis on *what* is being searched: see *Marakah*, *supra* note 3 at paras 16–20.

[57] *Riley*, *supra* note 11.

[58] *Ibid* at 10–15.

[59] *Ibid* at 2 and 8–22.

[60] *Ibid* at 2–3 and 10–12.

[61] *Ibid* at 4 and 22.

both the dissent and the USSC had held.[62] Justice Cromwell instead sought to justify the majority's approach by distinguishing device searches from strip searches.[63] The only other categorical exclusion from search incident to arrest the Court has recognized is the one set out in *Stillman*, prohibiting the collection of bodily samples on arrest.[64] While that was justified because such searches are always invasive, cell phone searches are only *potentially* so. Justice Cromwell was also optimistic that "meaningful limits"[65] could be placed on the search of electronic devices on arrest comparable to those imposed in the case of strip searches in *R v Golden*[66] – a case in which the majority held that strip searches are "inherently humiliating and degrading … regardless of the manner in which they are carried out".[67]

On behalf of the majority, Justice Cromwell then set out a test for when police can search a phone or digital device on arrest involving four conditions:

> (1) The arrest was lawful;
> (2) The search is truly incidental to the arrest in that the police have a reason based on a valid law enforcement purpose to conduct the search, and that reason is objectively reasonable. The valid law enforcement purposes in this context are:
> (a) Protecting the police, the accused, or the public;
> (b) Preserving evidence; or
> (c) Discovering evidence, including locating additional suspects, in situations in which the investigation will be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest;
> (3) The nature and the extent of the search are tailored to the purpose of the search; and
> (4) The police take detailed notes of what they have examined on the device and how it was searched.[68]

To be clear, the majority contemplated a limited search: "in practice", a suitably tailored search would involve "only recently sent or drafted emails, texts, photos and the call log".[69] Justice Cromwell also added: "[b]ut these are not rules, and other searches may in some circumstances be justified. The test is whether the nature

---

[62] Tim Quigley, "*R v Fearon*: A Problematic Decision" (2015) 15 CR (7th) 281 at 283.

[63] *Fearon*, *supra* note 5 at paras 60–62.

[64] *Stillman*, *supra* note 24.

[65] *Fearon*, *supra* note 5 at para 62.

[66] *Golden*, *supra* note 24.

[67] *Fearon*, *supra* note 5 at para 62, citing *Golden*, *supra* note 24 at para 90.

[68] *Fearon*, *supra* note 5 at para 83.

[69] *Ibid* at para 76.

and extent of the search are tailored to the purpose for which the search may lawfully be conducted."[70]

The majority was thus reluctant to set out a clear and categorical rule, and content to have the validity of device searches assessed after the fact. It is difficult to reconcile this with *Vu*. Justice Cromwell in that case cited *Hunter* for the point that protecting against unreasonable intrusions requires a means of preventing them before they occur.[71] In the case of computers, the Court held that this "calls for a specific assessment of 'whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding'".[72] In *Fearon*, this assessment could now be carried out by police officers and only after-the-fact by courts.

Justice Karakatsanis, joined by Justices Abella and LeBel in dissent, held the majority's test was "overly complicated" and called instead for a rule that is "clear, practical and effective."[73] Largely consistent with *Riley*, the dissent held that a reasonable device search on arrest required a warrant, except in cases of exigent circumstances. The latter would require reasonable suspicion of an imminent safety threat, or reasonable belief that it would prevent the imminent loss or destruction of evidence.[74] The difference of opinion as to how to strike the right balance here turned on a higher value the dissent placed on the privacy interests at issue. Faithful to the Court's reasoning on privacy in computers from *Morelli* to *Vu*, Justice Karakatsanis sought to apply this to the arrest context by drawing comparisons to the home and to the body:

> 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.[75]

---

[70] *Ibid*. One important proviso, at para 78, was that "generally, the search of the entire contents of a cell phone or a download of its contents is not permitted as a search incident to arrest". See also Nader Hasan, "A Step Forward or Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age" (2015) 71 SCLR (2d) 439 at 441, arguing that "the only way to achieve meaningful after-the-fact review is to require that police electronically record all warrantless cell phone searches."

[71] *Vu*, *supra* note 7 at para 46, citing *Hunter*, *supra* note 16 at 160.

[72] *Vu*, *supra* note 7 at para 47, citing *Hunter*, *supra* note 16 at 159–60.

[73] *Fearon*, *supra* note 5 at para 105.

[74] *Ibid* at paras 106, 179. At para 158: Even a search in these circumstances should "not extend that search beyond the scope of the grounds permitting the search".

[75] *Ibid* at para 152; see also para 101: "[p]rivate digital devices record not only our core biographical information but our conversations, photos, browsing interests, purchase records, and leisure pursuits. Our digital footprint is often enough to reconstruct the events of our lives, our relationships with others, our likes and dislikes, our fears, hopes, opinions, beliefs and ideas. Our digital devices are windows to our inner private lives."

A rule inviting police to carry out only cursory searches of recent texts and photos would not suffice, because it is "neither practical nor principled."[76] Agreeing with the US Supreme Court in *Riley* on this point, she held that giving police authority for "cursory searches" would readily lead to infringements, and be no less invasive than allowing police to conduct a warrantless "cursory walk inside a suspect's home."[77]

The majority's test would also "generate uncertainty for the police and result in increased after-the-fact litigation of searches" and "increased numbers of searches that were later determined to be unconstitutional."[78] Justice Karakatsanis was critical of the role police were asked to play here:

> Fundamentally, my colleague's approach puts the balancing decision in the hands of the police. I doubt not that police officers faced with this decision would act in good faith, but I do not think that they are in the best position to determine "with great circumspection" whether the law enforcement objectives clearly outweigh the potentially significant intrusion on privacy in the search of a personal cell phone or computer (para. 80). If they are wrong, the subsequent *exclusion of the evidence will not remedy the initial privacy violation*.[79]

Even if a test were fashioned on the basis of reasonable belief, the problem of potentially irreparable invasions of privacy would remain:

> … the exclusion of the evidence obtained at a subsequent trial *does not render the search harmless*. The arrested person's privacy will have been unjustifiably infringed, and their general sense of freedom and security affected […]. Only a requirement of pre-authorization *can give people* confidence that their privacy will be respected.[80]

---

[76] *Ibid* at para 162.

[77] *Ibid* at para 163. See also *Riley, supra* note 11 at 23–24. Critical reception of *Fearon* concurred. Tim Quigley, *supra* note 62, noted at 282: "The third requirement is extremely loose. Even a clear rule stipulating that only recent items may be examined begs the question of what is recent — and the police have been given the role of deciding that question. the additional qualification, at paragraph 76, that more extensive searches may sometimes be justified, is more distressing. No guidance has been given for when a cell phone search may be more intrusive. This places the police in the predicament of attempting to predict when they may search more extensively, but it also invites, rather than constrains, these further searches because the Court has explicitly said that it may approve them."

[78] *Fearon*, *supra* note 5 at para 164.

[79] *Ibid* at para 172 [emphasis added].

[80] *Ibid* at para 169 [emphasis added].

Citing the Court's earlier decisions in *Dyment*[81] and *Hunter*,[82] Justice Karakatsanis affirmed the point that adequately protecting privacy requires a means of preventing unjustified searches before they occur.[83]

The majority found the searches of Fearon's phone to violate section 8, but given the limited nature of the search and the compelling interest in locating the gun depicted in the photo, the evidence was admitted. The dissent viewed the impact of the breaches as "very serious" and held that the evidence should be excluded.[84]

Assessing the impact of *Fearon*

It is beyond the scope of this paper to examine post-*Fearon* case law in detail to assess the effectiveness of the majority's test. It may also be too early to attempt this. A search on canlii.org for citations to the Supreme Court's decision in *Fearon* brings up 132 cases at present, but few involve searches that took place after the Court's decision was published in December of 2014. However, I briefly draw on case law here to support the dissent's concern in *Fearon* that the majority's rule fails to provide clear guidance to the police, giving rise to what can be profoundly invasive searches. I begin with the first point – *Fearon* as a guide.

R v Moreau[85] concerned a search in December of 2015. Police found a phone on the accused when arresting him for drug possession. On the suspicion that he might also have been involved in a weapons offence, the officer searched the phone, examining a series of pictures, looking for "'trophy pics'" that he believed to be common in gun offence cases.[86] The court held the search to be unlawful for not being truly incident to arrest (the purpose being drugs not weapons) and excluded the evidence at issue. The case is unclear as to the extent of the officer's understanding of the rule in *Fearon*. But it invites consideration of whether the search would have unfolded had the Supreme Court's rule in *Fearon* been categorical (no phone search without a warrant, except in exigent circumstances).

A similar error occurred in *R v Kossick*.[87] In August of 2016, police seized a phone when arresting the accused for drug possession. Placing the phone in the front area of his cruiser, the officer saw incoming messages appearing on screen, suggesting involvement in trafficking. A few minutes later, at the detachment, the officer carried out a more extensive search of the device for further evidence of trafficking. The court

[81] *R v Dyment* [1988] 2 SCR 417, 55 DLR (4th) 503.

[82] *Hunter*, *supra* note 16.

[83] *Fearon*, *supra* note 5 at 169, citing Justice La Forest in *Dyment*, *supra* note 81 at 430; and *Hunter*, *ibid* at 160.

[84] *Fearon*, *supra* note 5 at paras 191 and 197.

[85] *R v Moreau*, 2016 ONCJ 564, 133 WCB (2d) 166.

[86] *Ibid* at para 12.

[87] *R v Kossick*, 2017 SKPC 67, 141 WCB (2d) 578.

held that neither search was truly incidental to arrest given that the arrest was for possession. It was also contrary to the rule in *Fearon* in that a search to discover evidence is only allowed where the investigation will be significantly hampered otherwise, which was not the case here. Once again, the facts invite consideration of whether the second, more extensive search would have unfolded had the rule in *Fearon* been categorical.

A third example can be found in *R v Goodwin*,[88] pertaining to a search that unfolded in January of 2015. Police carried out a "cursory" search of Facebook messages on the accused's phone at the station, roughly an hour after his arrest for trafficking. The officers testified that their purpose was discovery, but the court held there to be insufficient evidence that the investigation would have been significantly hampered without a prompt search.[89] While there was "some effort by the police to document what they were doing by way of screen shots that are really unreadable", this was held to be "the only place where Justice Cromwell's direction [in *Fearon*] was considered."[90] This might only be evidence of police lacking diligence or good training; but here too, it might also be read as the result of a rule that is "overly complicated."[91]

Case law also supports the dissent's concern in *Fearon* that a warrantless power to search devices on arrest would easily and readily lead to significant invasions of privacy not adequately remedied by the possibility of exclusion.

In *R v Wasilewski*,[92] the accused was charged with possession for the purpose of trafficking. Police seized her cellphone upon arrest and conducted a cursory search. Five days later, acting without a warrant, police conducted a more extensive search, including an inventory of some 2800 photos, many of which depicted the accused.[93]

In *R v Adeshina*,[94] the accused took issue with the police search of a phone found in a vehicle in which he was arrested for drug trafficking. Eight months after the arrest, police carried out a warrantless "data [dump]" of the entire content of the phone, resulting in some 682 pages of material.[95] The Court of Appeal for Saskatchewan considered the impact on the accused's privacy under section 24(2) of the *Charter* to be "severe."[96] The search revealed data on "the accused's personal choices in lifestyle

---

[88] *R v Goodwin*, 2016 NSSC 283, 134 WCB (2d) 239.

[89] *Ibid* at para 84.

[90] *Ibid*.

[91] *Fearon*, *supra* note 5 at para 105.

[92] *R v Wasilewski*, 2016 SKCA 112, 133 WCB (2d) 321 (overturning the trial judge's decision to exclude evidence).

[93] *Ibid* at para 7.

[94] *R v Adeshina*, 2013 SKQB 414, 110 WCB (2d) 836.

[95] *Ibid* at para 8.

[96] *Ibid* at para 34.

and adult 'XXX' movies, which he downloaded, as well as 'selfies', photos of the accused without his shirt on."[97]

In *R v Powell*,[98] police found a Blackberry on the accused when arresting him as a party to kidnapping and other serious charges. The device in this case was password protected. At the station an hour after the arrest, police gained access to and downloaded all of the data on the device in the form of a document amounting to some 3775 pages of material, including images, video, and text messages. An initial, cursory search of the material was held to be valid in exigent circumstances, but a more extensive search twelve days later (after the complainant had been rescued) was invalid, resulting in the exclusion under section 24(2) of the *Charter*.

Remedies for unlawful device searches on arrest

Where a device search violates section 8, exclusion is one remedy. But in casting doubt on whether this would be truly adequate in the case of a serious invasion of privacy, Justice Karakatsanis' comments raise an important issue: what other remedies or avenues of recourse are available in this context? A brief survey demonstrates that the options are few, relatively inaccessible, and of limited effect.

Damages under section 24(1) of the *Charter* are possible in theory, but are likely to be rare, due to procedural and substantive hurdles. The Supreme Court set out a five-part test for *Charter* damages in *Vancouver (City) v Ward*.[99] An applicant must first establish that a *Charter* right has been breached and why damages are a just and appropriate remedy, in terms of whether they would "fulfill one or more of the related functions of compensation, vindication of the rights, and/or deterrence of future breaches."[100] The burden then shifts to the state to demonstrate "countervailing factors [that] defeat the functional considerations that support a damage award", including the availability of an alternative remedy and concerns for good governance.[101] The Court did not specify that excluding evidence constitutes an alternative that renders damages redundant,[102] but lower courts have held this to be so.[103] Finally, the Court considers quantum.

---

[97] *Ibid*.

[98] *R v Powell*, 2017 ONSC 6482, 142 WCB (2d) 636.

[99] *Vancouver (City) v Ward*, 2010 SCC 27, [2010] 2 SCR 28 [*Ward*].

[100] *Ibid* at para 4.

[101] *Ibid.*

[102] *Ibid* at para 34.

[103] In *Ontario Society for the Prevention of Cruelty of Animals v. Hunter*, 2014 ONSC 6084 at para 53, 322 CRR (2d) 189, a case involving a 24(1) damages application for a section 8 breach, the court held that exclusion was an adequate remedy. *Hunter* was applied in *Abboud v Ottawa Police Services Board*, 2016 ONSC 1052, 265 ACWS (3d) 238, a case involving an application for damages under 24(1) for the search of a computer pursuant to an invalid warrant. Granting a summary motion to dismiss this part of the application, at paras 46 to 49, Smith J agreed with the defendant police board's submission that exclusion (resulting in acquittal) was "more responsive to the breach" of section 8 here, and also held that the plaintiff

Even if the *Ward* test were applied favourably, however, a damage award would likely be modest here. In *Ward* itself, the Supreme Court upheld the trial court's award of $5000 for a police station strip search in a case of mistaken identity. In a device case, the defendant would likely cite *Fearon* for the proposition that a device search is not inherently degrading or necessarily as invasive as a strip search.[104]

Procedurally, the Supreme Court in *Ward* indicated that "[p]rovincial criminal courts […] do not have the power to award damages under s. 24(1)."[105] In some provinces, small claims court has served as a venue for seeking a remedy under 24(1), but the awards have been modest.[106] The vast majority of case law on section 24(1) applications for damages pertain to superior court actions – a forum in which costs for counsel and disbursements are not trivial, and the risk of an adverse cost order is also an issue.

A further possible remedy is a tort action for breach of privacy. In four Canadian provinces, the tort is codified in a manner similar to section 1 of British Columbia *Privacy Act*, which states "[i]t is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another."[107] "Claim of right" here has been interpreted to mean "an honest belief in a state of facts which, if it existed, would be a legal justification or excuse."[108] At least one decision has recognized a claim of right in a matter involving a mistake of law.[109] Section 2 of

---

had failed to establish that "monetary damages are needed in order to compensate them or that monetary damages are required to highlight the harm that the breach caused to society… [or that] the police officers and Police Board must be deterred to ensure state compliance with the *Charter*." On this latter point, he noted, the plaintiffs "did not produce any evidence that the Police had a general practice of obtaining search warrants for residences without ensuring that they had reasonable and probable grounds to obtain a search warrant." See also, *Rotondo v Ottawa Police Services Board*, 2016 ONSC 8101, 275 ACWS (3d) 187, applying the reasoning in *Abboud* to another section 24(1) case relating to a section 8 breach, at paras 31 and 32.

[104] *Fearon*, *supra* note 5 at para 61.

[105] *Ward*, *supra* note 99 at para 58. See also *R v 974649 Ontario Inc (Dunedin)*, 2001 SCC 81, [2001] 3 SCR 575 at paras 56–59; and *R v Wetzel*, 2013 SKCA 143, [2014] 2 WWR 559, overturning a damage award granted in the course of a criminal trial in Provincial Court, citing both *Dunedin* and *Ward*.

[106] See, e.g. the Ontario Court of Justice (Small Claims) decisions in *Lamka v Waterloo Regional Police Services Board*, [2012] OJ No 5591, 2012 CarswellOnt 14587 (Ont SC), resulting in a $5000 award for an unlawful strip search, and *Probert v Galloway* 2011 CanLII 100790 (Ont SCSM), in which section 24(1) was considered but a remedy was granted under tort law; see also *AK v R*, 2014 NLPC 0113, 350 Nfld & PEIR 180, a case in which an order for costs was made as a section 24(1) remedy.

[107] *Privacy Act*, RSBC c 373, s 1(1) (British Columbia); see also *The Privacy Act*, RSS 1978, c P-24, s 2 (Saskatchewan); *Privacy Act*, RSNL 1990, c P-22, s 3(1) (Newfoundland & Labrador); and *The Privacy Act*, CCSM c P125, s 2(1) (Manitoba). On the scope and differences between the Acts, see Chris Hunt & Nikta Shirazian, "Canada's Statutory Privacy Torts in Commonwealth Perspective" (2016) Oxford U Comparative L Forum 3, online: <ouclf.isucomp.org/articles/>; see also Chris Hunt, "The Common Law's Hodgepodge Protection of Privacy" (2015) 66 UNBLJ 161.

[108] *Davis v McArthur*, 10 DLR (3d) 250 at 253, [1969] BCJ No 249 (QL), citing Boyd, C in *Rex v Johnson* (1904) 7 OLR 525 at 530, 24 CLT 266; cited affirmatively by the Court of Appeal in *Hollinsworth v BCTV* (1998), 59 BCLR (3d) 121, 83 ACWS (3d) 525 (CA) and noted in Hunt and Shirazian, *ibid*.

[109] *Peters-Brown v Regina District Health Board*, 136 Sask R 126, [1996], 1 WWR 337 (QB).

the BC *Privacy Act* further complicates the issue of police liability (in ways similar to other legislation) by excluding the conduct of a "peace officer acting in the course of his or her duty to prevent, discover or investigate crime" where privacy infringing conduct is not "disproportionate to the gravity of the crime or matter".[110] Thus, for example, in an investigation for trafficking or fraud, even if police carry out an invasive device search following an unlawful arrest – in flagrant breach of *Fearon* – a tort claim may be barred because police acted under a reasonable *suspicion*. Section 4 restricts actions under the Act to the province's superior courts, giving rise to the same monetary considerations noted above.

The common law tort of invasion of privacy presents further challenges. As defined by the Ontario Court of Appeal in *Jones v Tsige*,[111] a trier of fact would need to conclude that the search of a device constituted an intrusion upon a person's private affairs that would be "highly offensive to a reasonable person."[112] The plaintiff must establish intentional or reckless conduct, the lack of lawful justification, and that a "reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish."[113] The scope of "lawful justification" in the case of a device search is unclear; it might be interpreted strictly, but it might also afford a police service a defence where officers misapply *Fearon* but act in good faith.

Finally, the subject of an unlawful and invasive device search might complain to a police complaints commission or the federal or provincial privacy commissioner. A person might choose to make a complaint to a police oversight body where concerns about a search focus on the fact that sensitive data had been accessed, rather than that new records have been created or disclosed (*i.e.*, device data had been copied). In this case, a complaint could lead to discipline of officers involved and/or recommendations.[114] By contrast, a complaint would be made to a provincial or federal privacy commissioner where records have been "collected" in relation to one's personal data (*e.g.*, copies of data on a device were created and retained and possibly shared). On the basis of misuse or over-collection of one's personal information, a

---

[110] *Privacy Act*, RSBC C 373, *supra* note 107, s 2. See also s. 4(1)(d) of the Saskatchewan *Privacy Act, supra* note 107; s. 5(1)(d) of the Newfoundland *Privacy Act, supra* note 107; s. 5(e) of the Manitoba *Privacy Act, supra* note 107.

[111] *Jones v Tsige*, 2012 ONCA 32, 346 DLR (4th) 34.

[112] *Ibid* at para 70.

[113] *Ibid* at para 71.

[114] In the case of an RCMP officer, a complaint is first investigated internally, which may result in a disciplinary order under s. 45 of the *RCMP Act*, RSC 1985, c R-10. A complaint may also result in an external review under Part VI and VII of the *Act* by the Civilian Review and Complaints Commission for the RCMP. The CRCC's investigation may result in a report and recommendations to the RCMP Commissioner and possibly also the Minister of Public Safety. A complaint to the British Columbia Police Complaints Commissioner under the *Police Act*, RSBC 1996, c 367, which applies to forces other than the RCMP, can result, under Part 11 of the *Act*, in the imposition of disciplinary measures including training, suspension without pay, or ultimately dismissal. See the comparable disciplinary measures in section 85 of Ontario's *Police Services Act*, RSO 1990, c P 15.

privacy commissioner may have the power to order the records destroyed, in addition to making recommendations.[115]

The avenues of redress canvassed here are not easily accessed, or limited in terms of their potential effect. Realistically, in the case of an unlawful and invasive device search that does *not* proceed to prosecution, a meaningful remedy is unlikely. Where the matter does proceed to prosecution and evidence is excluded under section 24(2) of the *Charter*, the cases noted earlier demonstrate ways in which exclusion serves as only a partial remedy for what can be a significant violation of a person's dignity.

Legislation governing the powers of provincial and federal privacy commissioners might be amended to empower commissioners to award damages for violations of statutory privacy rights, as privacy advocates have urged in the past.[116] A preferable course, however, would be to return to the fork in the road the Supreme Court faced in *Fearon*, where the majority took a more questionable route. Not only was the majority's test inconsistent with the computer cases from *Morelli* to *Vu*, it also rested on speculative and dubious assumptions about the utility of immediate access to data. The US Supreme Court made a more prudent decision in imposing a categorical rule. The Court in *Riley* cited its earlier decision in *Michigan v Summers* for the proposition that "[i]f police are to have workable rules, the balancing of the competing interests […] 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'"[117] As technology continues to advance and breaches flowing from the confusion around *Fearon* continue to occur, the Supreme Court might have cause to reconsider its position sooner than it might otherwise.[118]

---

[115] For example, in British Columbia, where a person's data has been downloaded or copied from a person digital device by a non-RCMP police officer unlawfully, one might argue that the BC Privacy Commissioner would have jurisdiction to investigate a complaint for the improper "collection" of personal data, contrary to s. 2(d) of the British Columbia *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165. In the cases contemplated here, one might argue that an unlawful phone search does not fall within the "law enforcement" justification for the collection in s. 26(b) of the *Act* and that exclusion in s. 3(h) of the act for "a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed" would not apply to data gathered in the course of a prosecution which bore no "relation" or relevance to it. The Commissioner can issue an order to destroy records under s. 58(3)(f). For analogous provisions in Ontario, see ss. 39, 41, and 59(b)(ii) of the *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F 31; see also the *Privacy Act*, RSC, 1985 c P-21, ss. 3, 4, and 29.

[116] See, e.g. Office of the Privacy Commissioner of Canada, *The Case for Reforming the Personal Information Protection and Electronic Documents Act,* (Ottawa: Office of the Privacy Commissioner of Canada, May 2013) at 7.

[117] *Michigan v Summers*, 452 US 692 (1981) at 705, n 19, 101 S Ct 2587 (quoting *Dunaway v New York*, 442 US 200 (1979) at 219–220, 99 S Ct 2248 (White J concurring)), cited in *Riley*, *supra* note 11 at 22.

[118] For an argument calling into question whether the Court's analysis in *Fearon* was already rendered obsolete by technology appearing when it was decided, see Fehr & Biden, *supra* note 43. The authors write, at 100, that "identity protection functions," such as touch and face-ID, "raise additional constitutional concerns about the rights to silence and against self-incrimination, as well as provide additional privacy interests that were not given weight by either the majority or the dissent in *Fearon*."

Part II: Device searches at the border

The Canada Border Services Agency (CBSA) is authorized to carry out searches under various pieces of legislation, including the *Criminal Code*,[119] the *Immigration and Refugee Protection Act*,[120] and the *Customs Act*.[121] The focus in this section is on its powers under the latter Act. I begin with the legal framework supporting the CBSA's current claim to authority to search devices at the border, without a warrant and without grounds. I cite evidence to demonstrate the practical effect of these searches. I then discuss an emerging consensus around the need to add a requirement for reasonable suspicion. I conclude by arguing that a reasonable search under search 8 of the *Charter* requires a warrant on probable grounds.

The cornerstone of CBSA's argument as to the legality of its search of devices at the border is the Supreme Court's decision in *R v Simmons*,[122] which is the leading authority on search at the border. *Simmons* dealt with a challenge to strip search provisions in an earlier version of the *Customs Act*. Chief Justice Dickson held that:

> the degree of personal privacy reasonably expected at customs is lower than in most other situations. People do not expect to be able to cross international borders free from scrutiny. It is commonly accepted that sovereign states have the right to control both who and what enter their boundaries.[123]

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."[124]

Chief Justice Dickson then set out a framework for assessing searches at the border which is foundational to later jurisprudence:

> It is, I think, of importance that the cases and the literature seem to recognize three distinct types of border search. First is the routine of questioning which every traveller undergoes at a port of entry, accompanied in some cases by a search of baggage and perhaps a pat or frisk of outer clothing. No stigma is attached to being one of the thousands of travellers who are daily routinely checked in that manner upon entry to Canada and no constitutional issues are raised. It would be absurd to suggest that a person in such circumstances is detained in a constitutional sense and therefore entitled to be advised of his or her right to counsel. The second type of border search is the strip or

[119] *Criminal Code*, RSC 1985, c C-46.

[120] *Immigration and Refugee Protection Act*, SC 2001, c 27 [*IRPA*].

[121] *Customs Act*, *supra* note 13.

[122] *R v Simmons*, [1988] 2 SCR 495, 55 DLR (4th) 673 [*Simmons*].

[123] *Ibid* at para 49.

[124] *Ibid* at para 48.

> skin search of the nature of that to which the present appellant was subjected, conducted in a private room, after a secondary examination and with the permission of a customs officer in authority. The third and most highly intrusive type of search is that sometimes referred to as the body cavity search, in which customs officers have recourse to medical doctors, to X-rays, to emetics, and to other highly invasive means.[125]

The Court in this case was concerned with a search of the second type.[126] Strip searches on reasonable suspicion were held to be reasonable under section 8 in light of the compelling state interest in policing the border, especially "illicit narcotics trafficking",[127] as well as other safeguards in the Act, including provision for a second opinion on reasonable grounds from a superior officer.[128] In setting out this framework, however, the Court also affirmed the validity of cursory searches of a person and their goods without grounds or a warrant.

Later courts have added important glosses to the *Simmons* framework that are relevant here. In *R v Hudson*,[129] the Ontario Court of Appeal 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."[130] Courts have also distinguished between a "secondary search", or one that takes place at a remove from the main passageway in a border area, and a search of the second type contemplated in *Simmons*.[131] Case law on the scope of a category 1 search in *Simmons* is copious, but the boundaries are unclear. Among the examples of what is permissible, aside from a frisk or pat-down search, are a cursory search of baggage or

---

[125] *Ibid* at para 27. Dickson CJC'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, e.g. *R v Jones*, 81 OR (3d) 481, 41 CR (6th) 84 (Ont CA), holding there to be no REP at stage 1, and *R v Nagle*, 2012 BCCA 373, 266 CRR (2d) 257 applying a section 8 analysis to a stage 1 search.) See Robert Currie, "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14:2 CJLT 289 at 302 [Currie, Electronic Devices at the Border], who suggests that Dickson CJC 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 s. 8 analysis, beginning with *R v Edwards*, [1996] 1 SCR 128, 132 DLR (4th) 31 in which REP is determined as a threshold question for s. 8.

[126] *Simmons*, *supra* note 122 at para 28; Dickson CJC added a proviso 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."

[127] *Ibid* at para 52.

[128] *Ibid* at para 54.

[129] *R v Hudson* (2005), 77 OR (3d) 561, 137 CRR (2d) 215 (Ont CA) [*Hudson*].

[130] *Ibid* at para 30.

[131] *Dehghani v Canada (Minister of Employment and Immigration)*, [1993] 1 SCR 1053, 101 DLR (4th) 654.

purses, pockets, and the tapping of exterior parts of a car or truck to detect a hidden compartment.[132]

The CBSA claims authority to search a device and its data under sections 99(1)(a) and 99.3(1) of the *Customs Act*.[133] The argument is twofold. Section 99(1)(a) allows an officer to "examine any goods that have been imported"; 99.3(1) permits a "non-intrusive examination of goods" in "custody or possession" of a person in a "customs controlled area."[134] Section 2 of the Act defines "goods" to include "any document in any form", and data on a device is considered a "document".[135] A number of trial courts across Canada have agreed with this interpretation, holding section 99(1)(a) or 99.3(1) (or both) to be sufficient authority for device searches.[136] 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-intrusive" if performed pursuant to 99.3(1) (which applies only in a "customs controlled area").[137] 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 a purse.[138]

In June of 2015, the CBSA issued an internal Operational Bulletin that sheds further light on its legal position and practices. Titled "Examination of Digital Devices and Media at the Port of Entry – Guidelines",[139] the document begins by asserting that

---

[132] *Hudson, supra* note 129; *R v Sekhon*, 2009 BCCA 187, 189 CRR (2d) 176.

[133] *Customs Act*, *supra* note 13.

[134] *Ibid*, ss. 99(1)(a), 99.3(1). The *Customs Act* was amended in 2001 and in 2009 to allow for the designation and implementation of a "customs controlled area" (CCA) to address concerns about airport staff colluding with organized crime in illicit conduct. Within a CCA, both travelers and staff can be searched. An area of an airport or port of entry can be designated under regulation as a CCA, and several have been designated thus far: see the list at <https://www.cbsa-asfc.gc.ca/security-securite/cca-zcd/menu-cca-zcd-eng.html>, which 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, Regulatory Impact Analysis Statement, (2013) C Gaz II, 1834.

[135] *Customs Act*, *supra* note 13, s 2.

[136] *R v Gibson*, 2017 BCPC 237 at paras 94–98, 141 WCB (2d) 238 [*Gibson*]; *R v Buss*, 2014 BCPC 16 at para 25-31, 301 CRR (2d) 309 [*Buss*]; *R v Moroz*, 2012 ONSC 5642 at paras 20–22, [2012] OJ No 4843 [*Moroz*]; and *R v Saikaley*, 2012 ONSC 6794 at paras 79–82, OJ No 6024 [*Saikaley*]; *R v Whittaker*, 2010 NBPC 32 at para 8, 367 NBR (2d) 334; *R v Mozo* (2010), 316 Nfld & PEIR 304 at para 34; 2010 CarswellNfld 447 (NL Prov Ct) [*Mozo*]; and *R v Leask*, 2008 ONCJ 25 at para 7 and note 3, 167 CRR (2d) 267. 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. This was likely an error premised on a misunderstanding of the term "customs controlled area" (contained in s. 99.3(1)). Addressing this point at 19, Judge Kennedy wrote: "After hearing all the evidence, I am satisfied that the presence of the BSOs conducting an inspection/search of the vessel in the context of how the inspection took place is sufficient to conclude that the area of the inspection/search was a controlled area."

[137] *Customs Act*, *supra* note 13 at s. 99.3(1).

[138] See, e.g. *Buss*, *supra* note 136 at para 30; *Gibson*, *supra* note 136 at para 198.

[139] Canada Border Services Agency, "Examination of Digital Devices and Media at the Port of Entry – Guidelines", Operational Bulletin PRG-2015-31 (30 June 2015) [Guidelines]. The Guidelines came to light through an access to information reported by the BC Civil Liberties Association in August of 2016, but the Ministry of Public Safety confirmed its currency in February of 2017, as did Martin Bolduc, Vice-President

CBSA officials have authority under section 99(1)(a) of the *Customs Act* to examine device data as a form of "good" under section 2 of the Act.[140] It also cites section 139(1) of the *Immigration and Refugee Protection Act*[141] as additional authority for a device search. This section allows for a search of "personal effects" where there are reasonable grounds to believe a person has "not revealed their identity or has hidden on or about their person documents that are relevant to their admissibility".[142] But the Guidelines proceed to call for restraint in the exercise of these powers, indicating 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.[143]

The Guidelines also require a "clear nexus to administering or enforcing CBSA-mandated program legislation"[144] and that "[t]he officer's notes shall clearly articulate the types of data examined, and their reason for doing so."[145] A "multiplicity of indicators" may also authorize "progressive examinations of digital devices".[146] Officers must disable wireless radios on a device before proceeding to search, and if a traveler refuses a password, the device may be detained under section 101 of the Act.[147] The officers are advised that "[u]ntil further instructions are issued," they are not to arrest a traveler for refusing.[148]

There is some evidence, however, that the Guidelines are not being applied strictly – that searches are more routine than the document implies – and the searches

---

of CBSA's Programs Branch in submissions to Parliament in September of 2017. See Michael Vonn, "What Happens If You Don't Provide Your Cellphone Password to Border Agents?" (25 August 2016), *British Columbia Civil Liberties Association* (blog), online: <https://bccla.org/2016/08/what-happens-if-you-dont-provide-your-cellphone-password-to-border-agents/>; Matthew Braga, "Canadian Policies on Cellphone Searches at Border Aren't Easy to Find", *CBC News* (17 February 2017), online: <www.cbc.ca/news> [Braga, "Policies on Cellphone Searches"]; and Matthew Braga, "Canada's Border Agency to Start Tracking the Number of Cellphone Searches", *CBC News* (28 September 2017), online: <www.cbc.ca/news> [Braga, "Tracking Cellphone Searches"]. A more recent but amended version can be found online < https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf >.

[140] Guidelines, *supra* note 139 at 1.

[141] *IRPA*, *supra* note 120.

[142] *Ibid* at s. 139(1).

[143] Guidelines, *supra* note 139 at 1 [emphasis added].

[144] *Ibid* at 1.

[145] *Ibid* at 2.

[146] *Ibid*.

[147] *Ibid* at 3, 4.

[148] *Ibid* at 4. The full passage reads: "Until further instructions are issued, CBSA officers shall not arrest a traveller for hindering (Section 153.1 of the *Customs A*ct) 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."

are often invasive. In the 2017 British Columbia Provincial Court decision of *R v Gibson*,[149] two CBSA officers testified in some detail about their general practice in relation to the search of devices. The searches in this case took place in November 2014 (pre-dating the Guidelines) at the Pacific Highway border crossing in Surrey, British Columbia – but the trial took place in March and November of 2016.[150] Notably, Border Security Officers Randhawa and Louis speak of their general practice in relation to devices in the present tense. The accused, Gibson, had been referred to secondary inspection,[151] where the officers searched his phone, digital camera, and laptop. Associate Chief Judge Gillespie, summarizing Randhawa's evidence, stated that the officer believed that section 99(1)(a)

> permitted him to search electronic media for child pornography or anything that is illegal. He also understood that there were no limitations on what he could look for in reviewing the phone or camera. He was free to look at intimate pictures of people on phones and in media on other devices. BSO Randhawa testified that if he came across images where two adults were performing a consensual sexual act, he would not generally look at it, as, in his view, it was none of his business.[152]

Randhawa also testified that:

> he "regularly" inspects "people's Smartphones or iPhones", and that he does so in the course of a "routine Customs examination" looking for contraband, or anything that "indicates to us, basically, there is contraband, there is child porn, there is smuggling activity, or there is intelligence in regards to some sort of a – an offence that might occur on a later date."[153]

On the general routine of the search:

> [h]e would check messages looking to see if there was any history of messages about the "traveller's story". Then he would look at the images/photos on the phone. In the past, when he has reviewed the images he has found on cellular devices, he has observed "lots of illegal activity", such as people trafficking in drugs, taking photos of contraband drugs, and images of child pornography.[154]

---

[149] *Gibson, supra* note 136.

[150] *Ibid*.

[151] *Ibid* at para 9. Gibson was searched on the basis of suspicions raised by, among other things, the fact that he had taken a long bus journey across the United States only crossing in Vancouver, with the intention to stay for three days, that he was carrying a large amount of luggage and he was travelling on a new passport.

[152] *Ibid* at para 11.

[153] *Ibid* at para 15.

[154] *Ibid* at para 16.

Summarizing the evidence of the second officer, Louis, Justice Gillespie wrote:

> In the past, BSO Louis has reviewed hundreds of electronic devices at the border, perhaps in excess of a thousand. He generally approaches the review of [a] cellular device by looking at the messages to determine if they are consistent with the traveller's stated reason for entering the country. He looks at emails and text messages that have already been received and are stored on the phone itself. He does not have a specific practice about how far back he scrolls in the messages. Generally, he commences his review by examining the most recent ten to twenty messages. He also looks at the photos and videos that are stored on the device. He usually looks at the thumbnails of the images unless something specifically catches his eye. If he sees nothing that evidences a possible contravention under any of the Acts he enforces, he then concludes his examination.[155]

Louis is said to conduct "between five to twelve secondary examinations a shift" but that "[i]t was not 'one hundred percent routine for him to search a traveller's electronic media'".[156] There was no discussion of a "multiplicity of indicators" or any other grounds. The case makes no mention of the Guidelines.

This evidence is dated, impressionistic, and involves a very small sample. But it calls into question the practical effect of a standard as vague as "a multiplicity of indicators that may" point to contraventions. It also sheds light on the potential effect of a legal framework in which the scope of device searches is unlimited.

Charter concerns and proposals for reform

From the mid-2000s onward, courts have held that warrantless and groundless searches of devices under the *Customs Act* are reasonable.[157] Yet as Robert Currie has pointed out, a discrepancy begins to appear from *Morelli* onward, as courts have failed to effectively reconcile the Supreme Court's recognition of a heightened privacy interest in computers with the allowance in *Simmons* for cursory searches without grounds.[158] Arguments among defence counsel to the effect that the higher privacy interest calls for a standard of some kind have fallen flat. So too have concerns about groundless and limitless searches failing to perform the prophylactic function noted in *Hunter v Southam*[159] of avoiding unnecessary breaches before they occur.

Robert Currie has argued that while the privacy interest in a computer may not be as high as in a strip search, it remains high enough to call for distinct treatment

---

[155] *Ibid* at para 22.

[156] *Ibid* at para 23.

[157] See the cases cited in note 136.

[158] This would include *Moroz*, *Saikaley*, *Buss*, and *Gibson*, *supra* note 136. See also Currie, Electronic Devices at the Border, *supra* note 125 at 306.

[159] *Hunter*, *supra* note 16.

under the *Customs Act*. He proposes the Act be amended to make clear that data on a device is not "'goods'".[160] Drawing on the Supreme Court's sniffer dog cases as a framework (*R v Kang–Brown*,[161] *R v A.M.*,[162] and *R v Chehil*[163]), he proposes reading into sections 99(1)(a) and 99.3(1) a requirement for reasonable suspicion.[164] This is the requisite basis for other searches under the *Customs Act*, including a strip search.[165] He also proposes limiting the search to "the more basic apps on the device – sent and draft emails and texts, photos, call logs, note-taking apps and anything similar."[166]

In the fall of 2017, the House of Commons Standing Committee on Access to Information, Privacy and Ethics held hearings to address the issue of device searches at the border. The CBSA made submissions outlining its practices as set out in the 2015 Guidelines, including its requirement for a "multiplicity of indicators". In the course of hearings, the CBSA confirmed that it had not been keeping statistics about the number and nature of searches, but had begun to do so weeks earlier and would make this public in due course.[167] The Committee's report, tabled in December of 2017, acknowledges the thrust of recent Supreme Court jurisprudence on the high privacy interest in digital devices and concerns about the "lack of clear rules in the *Customs Act*."[168] But the Committee appears not to have probed the CBSA's position in much depth – omitting any discussion in the report of the Agency's need to conduct device searches, or the effectiveness of searches being conducted. The report also suggests a consensus around reasonable suspicion as an appropriate standard for device searches, though at least one witness proposed that a warrant be required.[169] Among the Committee's recommendations were that CBSA's 2015 Guidelines "be written into the *Customs Act*."[170] Yet the Committee also recommended that the standard of a "multiplicity of indicators" be replaced with "reasonable grounds to suspect."[171] A

---

[160] Currie, Electronic Devices at the Border, *supra* note 125 at 316.

[161] *R v Kang-Brown*, 2008 SCC 18, [2008] 1 SCR 456.

[162] *R v AM,* 2008 SCC 19, [2008] 1 SCR 569.

[163] *R v Chehil*, 2013 SCC 49, [2012] 3 SCR 220.

[164] Currie, Electronic Devices at the Border, *supra* note 125 at 310–11.

[165] *Customs Act*, *supra* note 13 at s. 99(1)(a).

[166] Currie, Electronic Devices at the Border, *supra* note 125 at 312.

[167] Braga, "Tracking Cellphone Searches", *supra* note 139.

[168] *Protecting Canadians' Privacy*, *supra* note 14 at 5.

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

[170] *Ibid* at 11.

[171] *Ibid*. Among the other recommendations was, at 13, 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. Another, at 22, 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."

further key recommendation was for the government to track the number of device searches and provide regular updates to the Privacy Commissioner of Canada.[172]

Recent events in the United States present a notable contrast to this approach. Device searches at the US border have been rising rapidly in recent years, causing concern among Americans.[173] In response, a bi-partisan bill, titled the *Protecting Data at the Border Act*, was tabled in Congress in April of 2017.[174] It requires border agents to obtain a warrant on probable grounds before searching a device. The bill would also prohibit denying entry for refusal to provide a password or unlock a device, require officers to notify travelers of the right to refuse requests to provide access, require probable grounds for confiscating a device, and prohibit the admission of evidence obtained in violation of the bill.[175] The bill is currently in committee stage in both chambers.

The bill represents a notable contrast to debates about law in Canada because it reflects a different set of assumptions about both privacy and the state interest in the search of a device at the border. A warrant requirement to conduct even a limited search implies a view – consistent with that set out in *Riley* – that the state's interest in immediate access to data in this context is not pressing. It also implies a view that the fruits of warrantless data searches at the border do not generally outweigh the privacy interests engaged in such searches. The bill sets out a concept of reasonable search premised on facts and assumptions that apply equally in Canada.

Why the reasonable search of a device should require a warrant, even at the border

The option of adopting the reasonable suspicion standard has much to commend it, including its consistency with other invasive searches in the *Customs Act*. But in what follows, I argue that section 8 of the *Charter* requires a warrant on probable grounds for device searches at the border, except in exigent circumstances. The argument is threefold.

First, the search of a device is close in nature to a strip search, and among the most invasive searches possible. This is consistent with the Supreme Court's holding in *Morelli* to *Vu*, and both the dissent *and* the majority in *Fearon.* On behalf of the

---

[172] *Ibid* at 13.

[173] US Customs and Border Protection, "CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics", (5 January 2018) noting 30 200 device searches for fiscal year 2017 – an increase from 8503 in 2015, and 19 033 in 2016. See also Kaveh Waddell, "The Steady Rise of Digital Border Searches", *The Atlantic* (12 April 2017), online: <www.theatlantic.com>, "the rate of digital border searches is in on pace to quadruple since 2015."

[174] US, Bill S 823, *Protecting Data at the Border Act,* 115th Cong 2017–2018; Adam Schwartz and Sophia Cope, "Pass the Protecting Data at the Border Act" (28 September 2017) *The Hill* (blog), online: <www.thehill.com>.

[175] *Ibid*.

majority in *Fearon*, Justice Cromwell did state that a device search is "not as invasive as a strip search."[176] But he did so at the end of his discussion of the differences between the two kinds of search. In the course of that discussion, his point was more nuanced: "while cell phone searches […] may constitute very significant intrusions of privacy, not every search is inevitably a significant intrusion."[177] Which is to say that some of them can be; further on, he conceded: "[a]ll of that said, the search of a cell phone has the potential to be a much more significant invasion of privacy than the typical search incident to arrest."[178] Justice Karakatsanis, in dissent, was more overt in asserting an equivalence between device and strip searches. She drew the analogy twice, including the claim that "like the search of a private home, a strip search or the seizure of bodily samples, the search of the portal to our digital existence is invasive and impacts major privacy interests. The privacy interest in a cell phone or other digital communication and storage device is extremely high."[179] Supreme Court authority clearly favours placing device searches very close to strip searches, or not far below them.

If a device search is close to a strip search, why should a device search at the border require more than reasonable suspicion when a strip search requires only that? The response is that a limited data search (tied to a law enforcement objective) is not practicable; and more crucially, the state interest in searching a device at the border is *lower* than it is in the search of a *person*.

Justice Karakatsanis was correct to assert in *Fearon* 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."[180] Since messages can be communicated through many different apps and platforms, an attempt to limit a search to recent messages or emails will likely still entail an inspection of "a host of applications" in a search that is "far from minimal and [an] inspection far from quick."[181] Moreover, "a cursory inspection of photos may involve any number of private and personal photographs of the individual—and of third parties."[182] The US Supreme Court in *Riley* cast a similar doubt on the merits of limited searches of devices, holding that such an approach would "impose few meaningful constraints on officers. The proposed categories would sweep in a great deal of information, and officers would not always be able to discern in advance what information would be found where."[183]

---

[176] *Fearon*, *supra* note 5 at para 63.

[177] *Ibid* at para 54.

[178] *Ibid* at para 58.

[179] *Ibid* at para 134. See also para 152, "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."

[180] *Ibid* at para 164.

[181] *Ibid*.

[182] *Ibid*.

[183] *Riley*, *supra* note 11 at 24.

More crucially, the state's interest in searching a device at the border is less pressing than it is in searching a person's body. In *Simmons*, Chief Justice Dickson accorded significant weight to the state interest in a strip search "[i]n light of the existing problems in controlling illicit narcotics trafficking and the important government interest in enforcing our customs laws".[184] Yet vital to this assessment was the simple fact that people often use their bodies as vessels for importing illicit goods. Whereas the state has a pressing need to carry out a strip search to prevent drug or weapons smuggling, the same cannot be said for child pornography or other illicit *data*.[185] Obviously, the vast majority of illicit data that enters Canada does so through the internet.[186] A cursory glance at the cases on device searches at the border will show that most involve accused persons of seemingly limited technical savvy caught in possession of relatively small amounts of child pornography – and thus not cases of sophisticated hackers who thought it best to physically import their data rather than use a virtual private network, a secured socket layer or encrypted tunnel, and so forth.[187] Nor is it clear from the case law that device searches are meaningfully assisting in the prevention of conventional customs violations by affording officers evidence pointing to drug or weapons trafficking offences. The state's interest in interception at the border is thus far less pressing and more speculative in any given case of a person carrying a device than it is where there is a reasonable suspicion of smuggling contraband.[188]

---

[184] *Simmons*, *supra* note 122 at para 52.

[185] A number of scholars have made this point in the Canadian and American contexts (and in the latter case, at least as far back as 2008). In relation to Canada, see Steven Penney, "'Mere Evidence'? Why Customs Searches of Digital Devices Violate Section 8 of the *Charter*" (2016) 49:1 UBC L Rev 485 at 510 [Penney, "Mere Evidence"]; in relation to the US, see Thomas Mann Miller, "Digital Border Searches After *Riley v. California*" (2015) 90 Wash L Rev 1943 at 1991–2; Janet C. Hoeffel and Stephen Singer, "Fear and Loathing at the U.S. Border" (2013) 82:4 Miss LJ 1 at 13; 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 at 1017; and 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 at 177.

[186] Penney, "Mere Evidence", *supra* note 185 at 510–11: "The overwhelming proportion of child pornography and other digital contraband moves through the internet, not customs. Even 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."

[187] There are, to my knowledge, nine reported decisions involving device searches at the border. Including the seven cases listed in *supra* note 136, two additional cases are *R v Appleton* (2011), 97 WCB (2d) 444, 2011 CarswellOnt 11191 (ONCJ), and *R v Bares*, 2008 CanLII 9367 (Ont Sup Ct) (involving the search of CDs rather than a device). Seven of the nine cases deal with searches that discover files containing child pornography; in *Appleton*, the search at issue involves a text message. In *Saikaley*, *supra* note 136, the CBSA recovers a debt list from a suspected drug-dealer's phone, but they were acting on information gleaned from a wiretap and an earlier investigation by the RCMP. I note that the list of device search cases in this paper is consistent with Robert Currie's inventory, *supra* note 125 at 300, with the addition of the more recent *R v Gibson*, *supra* note 136.

[188] One possible exception to this is the potential utility of a device search where border officers believe a person is concealing their identity. Even cursory details gleaned from a device search – the language of the operating system, the apps on the phone, etc. – could offer meaningful assistance in this case (including the traveler's past whereabouts). The power to search under section 139(1) of the *IRPA*, *supra* note 120, should thus be considered distinct from *Customs Act* powers. Yet given the high privacy interest involved in a device and the likelihood that a categorical rule would be a more effective means of avoiding unreasonable

It may seem counter-intuitive to assert that while a strip search can be carried out under the *Customs Act* on reasonable suspicion, a device search should require a warrant. But, to be clear, the difference is premised not on which search is more invasive, but rather which search is more *pressing.* Drug and weapons smuggling are common and can only occur physically. Body searches are often necessary to prevent these acts and often effective. The evidence of CBSA officials noted above (from *R v Gibson*) suggests that device searches are occurring frequently, yet the number of cases dealing with charges for illicit data captured in the course of device searches at the border is very small. CBSA officials are searching devices not because they serve an effective law enforcement purpose comparable to preventing drug or weapons smuggling, but because they assume it is a reasonable extension of their powers under the Act. No decided case in Canada has cited evidence as to the pressing need to carry out device searches at the border on the basis of the significant threat they pose as vessels for illicit material or their effectiveness in the aid of law enforcement.[189] These points are often made and rarely questioned.[190]

The *Customs Act* should thus be amended to allow for a device search only with a warrant on probable grounds, except in exigent circumstances.[191] The additional protections set out in the *Protecting Data at the Border Act*, noted above, would also be appropriate. The right to be free from an unreasonable device search would thus be better protected in Canada if the *Customs Act* were to include a prohibition on denying entry for refusing to provide a password; a requirement of probable grounds to seize a

---

searches, here too a warrant requirement would be preferable to the current requirement (under section 139) of reasonable grounds.

[189] And as noted above, nor did the Committee report, *Protecting Canadians' Privacy*, *supra* note 14. This may be due in part due to a lack of record keeping on the part of the CBSA, a situation that officials promised in the course 2017 Parliamentary hearings to rectify: Braga, "Tracking Cellphone Searches", *supra* note 139.

[190] There are a number of challenges unfolding in the United States to the validity of device searches at the border under the Fourth Amendment, including *Alasaad* v *Duke*, No 1:17-cv-11730 (Mass Dist Ct 2018) and *United States v Molina-Isidoro*, No. 17-50070 (5th Cir 2018). In both cases, the government makes the same assertion that CBSA makes here: i.e., that groundless searches are reasonable in light of the state interest in immediate access to data at the border. Yet the claim is seldom if ever substantiated. For example, among the documents cited in the government's materials in *Alasaad* is a 2018 US Customs and Border Protection directive which states that devices searches are "essential to enforcing the law […] They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography." US Customs and Border Protection, *Border Search of Electronic Devices* (CBP Directive No 3340-049A) (2018) at 1. Nowhere in the document is there evidence of the number of searches conducted or the amount of material found or its nature. Similar assertions about urgency and necessity are made without evidence in Homeland Security's more extensive 2018 update, US Customs and Border Protection, *Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices* (DHS/CBP/PIA-008(a) (January 4, 2018). For context on the cases, "ACLU & EFF Sue Over Warrantless Phone and Laptop Searches at U.S. Border" (13 September 2017), *ACLU* (blog), online: <www.aclu.org/news/aclu-eff-sue-over-warrantless-phone-and-laptop-searches-us-border; and Electronic Frontier Foundation> and "EFF to Court: Border Agents Need Warrants to Search Contents of Digital Devices" (8 August 2017), *EFF* (blog), online: < www.eff.org/press/releases/eff-court-border-agents-need-warrants-search-contents-digital-devices>.

[191] The exception for searches in exigent circumstances that Karakatsanis J set out for the dissent in *Fearon, supra* note 5 at para 179, would be appropriate here: reasonable suspicion of imminent harm; reasonable belief of imminent danger that evidence would be destroyed.

phone (pending a warrant on probable grounds); and strict limits on how long a device can be held without a warrant. Courts dealing with exclusion applications under section 24(2) of the *Charter*, in cases where phones have been unlawfully searched, should lend significant weight to the privacy interests in a device, in accordance with the Supreme Court's holdings from *Morelli* onward. Courts should generally be reluctant to admit evidence obtained from warrantless border device searches (contrary to section 8) where the searches are more than cursory (recent texts, emails, and photos).

Remedies for an unreasonable border search?

The prospect of an unlawful – or unreasonable – device search at the border presents a distinct set of concerns from those at issue in the context of search incident to arrest. In the latter case, a device searched on arrest may lead to a trial and a finding under section 8. The majority's test in *Fearon* will serve as a gauge for the legality of the search, forming a basis for assessing the severity of the breach in relation to police conduct. In addition to the exclusion of evidence, the subject of a search might in theory seek damages under section 24(1) of the *Charter*, or in tort, or make a complaint to a police oversight body or to a privacy commissioner.

The avenues for redress or a remedy in the case of an invasive and unreasonable device search at the border are less clear. Given that device searches can be lawfully conducted at present without grounds, there is no basis for damages under the *Charter* or in tort. There may, however, be a basis to complain about the conduct of CBSA officers in relation to the Guidelines noted above.[192] Serious intrusions into privacy are thus often occurring without recourse.

Part III: Conclusion

Current authority in Canadian law for device searches on arrest and at the border is inconsistent with the Supreme Court's holdings from *Morelli* onward on the privacy interest in computers. Adding to earlier criticism of *Fearon* and of current border device search law and policy, this paper has sought to demonstrate that searches are being carried out in both contexts without clear limits, leading to significantly invasive state intrusions into personal privacy, and without effective avenues of recourse. New technologies of data protection may soon provide the Supreme Court an opportunity to revisit its holding in *Fearon*.[193] If so, the Court should adopt the dissent's recommendation for a warrant except in exigent circumstances as a means of

[192] The Office of the Privacy Commissioner of Canada recommends that if one has concerns about the manner in which a search is carried out by CBS border agents – e.g. in a manner inconsistent with the Guidelines noted above – a person might submit comments through an online feedback and complaint form with the Canada border services agency at: <http://www.cbsa-asfc.gc.ca/contact/feedback-retroaction-eng.html>.

[193] Fehr & Biden, *supra* note 43.

addressing the dissent's concerns about the practical effects of the rule which this paper has sought to substantiate.

Parliament should amend the *Customs Act* to provide clearer guidance on CBSA authority for device searches at the border. But it should be skeptical of the CBSA's claims to having a *pressing* interest in data searches, comparable to its interest in physical searches. The salient point in this context is not whether a device search is less invasive than a strip search, but whether it is necessary or effective in ways comparable to a body or container search. Parliamentarians need to ask why border officials need *immediate* access to people's data, and what past practice in this regard has tended to reveal. If several years of a substantial number of searches has resulted in only a small number of cases, mostly involving child pornography, clearly the need to carry out immediate (warrantless) searches is more theoretical than practical. A reasonable search here – one that balances the high privacy interest in personal devices with a theoretical state interest in access *in the vast majority of cases* – is one that should require a warrant on probable grounds, except in exigent circumstances.

Until these reforms are adopted, invasive searches will continue to occur in both contexts and without accessible or effective remedies. In the absence of these changes to the law, it may be that, for many people, technology itself will offer the most effective solution to the concerns raised in this article, in the form of pass-locks and encryption.[194] But technology constantly evolves, and many devices continue to feature a level of access in the form of notifications and other data accessible without a passcode. Many people also continue to use their devices unlocked. There are thus various ways the state may gain access to device data on arrest or at the border despite attempts to avoid it. The constitutional protection of privacy therefore remains vital, and along with it, the need to constantly reassess the meaning of a reasonable search in the digital context.

[194] In the case of Apple, beginning with iOS 9, all content stored on iPhones and iPads has been encrypted, making it more difficult for law enforcement to gain access. Analogous protections have been added to other platforms. For an argument that encryption may offer the best defence against state incursions into digital privacy, see Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (New Haven: Yale University Press, 2017).