

ARTICLE

REASONABLENESS AS PROPORTIONALITY: TOWARDS A BETTER CONSTRUCTIVE INTERPRETATION OF THE LAW ON SEARCHING COMPUTERS IN CANADA

Agathon Fric*

CITED: (2016) 21 Appeal 59

INTRODUCTION.....	60
A. Method	61
B. Scope.....	62
I. COMPUTERS, PRIVACY & THE LAW IN CONTEXT	63
A. The Privacy Interests in Digital Information Are Unique	63
B. Assessing the Reasonableness of Searching Digital Information	64
II. SEARCHING ELECTRONIC DEVICES INCIDENT TO ARREST	67
A. Law as Integrity	68
B. A Poor Constructive Interpretation	69
III. SEARCHING ELECTRONIC DEVICES AT THE BORDER.....	73
A. Distinguishing <i>R v Fearon</i>	74
B. A Fourth Category?	75
C. The Border Fallacy	76
D. A Better Constructive Interpretation	78
E. Proportionality as Integrity.....	80
CONCLUSION	82

* Agathon Fric is a graduate of Dalhousie University's Schulich School of Law and holds a Bachelor of Arts (Honours) in Political Science from Carleton University. He is currently articling as a student-at-law with the Court of Queen's Bench of Alberta. Special thanks go to Professor Sheila Wildeman, without whose feedback and guidance this article would not have been written.

INTRODUCTION

It is axiomatic to suggest that the law tends to be a reactive force. Very rarely, or successfully, has the law been used to positively influence the behaviours of social actors until sufficient damage has been done to catapult an issue into the mainstream. Even when it does emerge, proactive regulation has traditionally been the domain of legislatures. Unlike courts, politicians are not obliged to justify their decisions on the basis of or in spite of what came before, freeing them to pursue whatever ends they wish, on any grounds whatsoever, subject only to the constitution. However, when one accounts for the exponential speed at which technology develops, legislatures do not fare much better at future-proofing their laws, and when the state's interest is arguably opposed to that of the individual, courts will necessarily be called upon to strike the balance. Case in point: on March 3, 2015, Canada Border Services Agency (“CBSA”) personnel at the Halifax Stanfield International Airport charged Alain Philippon, a Quebec man returning from a trip to the Dominican Republic, with hindering an official from doing something he was authorized to do under the federal *Customs Act*, namely to search any “goods” up to the time of the traveller's release at the border.¹ In particular, Philippon was alleged to have “hindered” the official's investigation by refusing to divulge the passcode that would unlock his Blackberry smartphone.² In November 2015, he pleaded not guilty and his trial was scheduled for August 2016.³ If convicted, Philippon faces a mandatory minimum \$1,000 fine with a maximum penalty of \$25,000 and 12 months of imprisonment.⁴ Had Philippon willingly disclosed his password, enabling border officers to search the contents of his phone, he would have been among the many travellers who have passively surrendered access to their personal electronic devices, either “not wanting any trouble” or “having nothing to hide.”⁵ However, news of Philippon's civil disobedience quickly spread around the world, making international headlines and leaving many Canadians wondering whether border agents actually have the legal authority to search their cell phones and, if so, whether that should be the case.

Section 8 of the *Canadian Charter of Rights and Freedoms* states: “Everyone has the right to be secure against unreasonable search or seizure.”⁶ The highly sensitive nature and sheer volume of information that computers, such as laptops, tablets, cellular phones, and other electronic devices, hold or have the ability to access remotely go to the “biographical core”⁷ of an individual and thus attract a reasonable expectation of privacy. Attempts by agents of the state to access that information constitute an infringement of this reasonable expectation of privacy. Where one has a reasonable expectation of privacy at law, an infringement of that reasonable expectation amounts to a “search” as that term has been interpreted under section 8.⁸ The search must then be “reasonable” in order to be upheld as constitutional. This much is clear.

1 *Customs Act*, RSC 1985, c 1 (2d Supp), ss 13, 99, 153.1.

2 Jack Julian, “Alain Philippon Phone Password Case May Meet Charter Challenge Conditions”, *CBC News* (7 March 2015), online: <<http://www.cbc.ca/news/canada/nova-scotia/alain-philippon-phone-password-case-may-meet-charter-challenge-conditions-1.2985694>> archived at <<https://perma.cc/2CTJ-Z78T>>.

3 Steve Bruce, “Quebec Man to Fight Customs Charge of Hindering”, *The Chronicle Herald* (5 November 2015), online: <<http://www.thechronicleherald.ca/metro/1320917-quebec-man-to-fight-customs-charge-of-hindering>> archived at <<https://perma.cc/H26K-62KX>>.

4 *Customs Act*, *supra* note 1, s 160.1.

5 See e.g. *R v Buss*, 2014 BCPC 16, 301 CRR (2d) 309 [Buss]. In this case, the accused gave border agents the passwords to his computer and cell phone, subsequently claiming that this violated the principle against self-incrimination under section 7 of the *Charter of Rights and Freedoms*.

6 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [Charter].

7 *R v Plant*, [1993] 3 SCR 281 at 293, 145 AR 104.

8 Stephen Coughlan, *Criminal Procedure*, 2nd ed (Toronto: Irwin Law, 2012) at 66.

Assessing reasonableness inherently calls upon courts to balance the interests of the state with those of the individual. However, existing common law jurisprudence governing the reasonableness of searching the contents of Canadians' personal electronic devices does *not* strike an appropriate balance between the individual's reasonable expectation of privacy and the state's interest in intruding upon that expectation to pursue the objectives of law enforcement. Most notably, the Supreme Court of Canada's majority judgment in *R v Fearon*⁹ does not sit comfortably alongside fundamental aspects of the legal record, contrary to legal philosopher Ronald Dworkin's theory of law as integrity. This suggests that a better constructive interpretation of the law is needed in order to determine the reasonableness of computer searches at customs, for instance by referring to how reasonableness is assessed in other constitutional contexts. Courts ought to apply a more robust proportionality analysis, like that developed under section 1 of the *Charter*, in order to demonstrate integrity and to make the law on search and seizure of electronic devices "the best that it can be."¹⁰

A. Method

This paper seeks to address the reasonableness and, by extension, the justness of searching the contents of electronic devices in a variety of contexts. It does this not from a normative, privacy-or-die mentality, but by starting with a proposition first advanced by Dworkin: that in the absence of complete agreement as to the justice or morality¹¹ of adopting a particular interpretation of the law, judges can, do, and should demonstrate their commitment to act morally by acting with integrity—that is, by striving for coherence in their decision-making. Coherence does not *guarantee* that judges are, in fact, acting justly. However, when courts act incoherently, it suggests that they will only act morally by happenstance.¹² Coherence is thus to be preferred.

The relative incoherence in the way that Canada currently treats the search and seizure of electronic devices cannot be fully justified on the basis of the different contexts in which they occur, necessitating this quest for a better constructive interpretation of the law on search and seizure. Firstly, the paper begins by situating the issue of search and seizure of electronic devices by the state in its current social and legal context. In particular, I highlight these devices' differential legal treatment inside homes, after arrest, and at national ports of entry, including land border crossings and airports. This summary surveys the relevant constitutional, statutory, and common law norms that have historically governed Canada's search and seizure practices in relation to computers.

Secondly, I use Dworkin's interpretive theory of adjudication in order to frame a critique of the search incident to arrest doctrine as it has been applied to electronic devices, specifically cell phones. At this juncture, it is fair to ask "Why Dworkin?" What can *his* theory add to the discussion? Aside from the fact that his legal philosophy has been among the most influential in the last century, law as integrity offers a rubric to critically assess the Supreme Court of Canada's (mal)treatment of electronic devices searched incident to arrest. I therefore closely track the written reasons of the majority decision in *R v Fearon*, challenging the degree to which Justice Cromwell's constructive interpretation can be meaningfully described in Dworkinian terms as "fitting" or "justifying" the law on search and seizure as a whole. However, if Dworkin's interpretive theory is the stone that creates a chink in search and seizure law's armour, its real power lies in its ability to reconcile my central proposal here—that the doctrines of search incident to arrest

9 *R v Fearon*, 2014 SCC 77, [2014] SCR 621 [*Fearon*].

10 Ronald Dworkin, *Law's Empire* (Cambridge: Harvard UP, 1986) at 229.

11 I use these terms interchangeably.

12 Scott Hershovitz, "Integrity and Stare Decisis" in Scott Hershovitz, ed, *Exploring Law's Empire: The Jurisprudence of Ronald Dworkin* (New York: Oxford UP, 2006) 103 at 115–116.

and the so-called “border exception” need refinement in light of the heightened privacy interests engaged by the contents of an individual’s digital devices—with seemingly contradictory precedent. As this article will demonstrate, Dworkin’s interpretive theory gives courts a licence to correct mistakes of the past without sustaining indecent attacks on their—and the law’s—integrity.

Thirdly, after establishing that the Supreme Court of Canada’s approach to electronic devices in the search incident to arrest context fails to provide the best constructive interpretation of the law as a whole, I consider how this lesson can and should inform the law’s development in the border context. This analysis draws from the Supreme Court of Canada’s jurisprudence on the “reasonable limits” clause at section 1 of the *Canadian Charter of Rights and Freedoms*, as well as the Court’s more recent application of a “robust” reasonableness standard in discretionary administrative decisions that engage *Charter* protections.¹³ Lastly, I offer proportionality theory as a potential lodestar for assessing the reasonableness of a law that authorizes computer searches by customs officials without any reasonable grounds.

B. Scope

Strictly speaking, this paper is not about the admissibility of evidence discovered in violation of section 8 of the *Charter*, which may be excluded under section 24(2).¹⁴ While this essay addresses the search and seizure of computers at the Canadian border, it considers only digital content-related searches of such devices. That does not include physical searches of an electronic device in order to satisfy border officers that it is not concealing drugs or other non-digital contraband. It is also beyond the scope of the present analysis to answer whether and under what circumstances a CBSA officer may or may not compel a traveller such as Philippon to divulge his password or to otherwise actively assist the agent in the inspection of the traveller’s electronic devices. This is an interesting question worthy of independent inquiry;¹⁵ however, this second-order question assumes in the first place that the right of a border officer to search digital devices without individualized suspicion or probable grounds has been settled in law now and forever.¹⁶ It is to this preliminary question that this analysis turns its attention: does the treatment of computers as “goods” like any others under the *Customs Act* constitute a reasonable limit on one’s reasonable expectation of privacy in the contents of these devices? Put differently, does the uniform treatment of a computer and a briefcase at the border strike an appropriate balance between the state and individual interests at stake in an unwarranted search of those items? I argue that proportionality theory, variously

13 *Charter* “protections” encompass specific rights, as well as more ambiguous (and undefined) values. See *Loyola High School v Quebec (AG)*, 2015 SCC 12, [2015] 1 SCR 613 [*Loyola*]; *Doré v Barreau du Québec*, 2012 SCC 12, [2012] 1 SCR 395 [*Doré*].

14 For the appropriate test on admissibility, see *R v Grant*, 2009 SCC 32, [2009] 2 SCR 353 [*Grant*].

15 It has received some cursory treatment: see Robert Currie, “Cell Phone Searches at the Border: A New Frontier” (13 March 2015), *International & Transnational Criminal Law* (blog), online: <<http://rjcurrie.typepad.com/international-and-transna/2015/03/cell-phone-searches-at-the-border-a-new-frontier.html>> archived at <<https://perma.cc/J5VS-3UEL>>; *Buss*, *supra* note 5 at 33. An answer to this question may also be inferred by analogy from *R v Cimini*, [2008] OJ No 5380 (Ont Ct J) at paras 17–18: “If locked and the person refused to produce the key and the police are unable to access the trunk or glove box without the key then inaction in refusing to produce the key to access the trunk of the vehicle could amount to hindering or preventing” [emphasis added]. On this reading, it would appear that the Crown must prove customs officials took positive steps to try to unlock Philippon’s phone without his help before it could reasonably charge him with hindering or preventing a Canada Border Services Officer from completing her duties under section 153.1 of the *Customs Act*. Of course, this assumes no distinction is to be drawn between digital devices and traditional receptacles, which runs counter to the spirit of this essay and the jurisprudence.

16 Indeed, it would appear that way on a strict interpretation of *R v Simmons*, [1988] 2 SCR 495, 55 DLR (4th) 673 [*Simmons*].

invoked by the Supreme Court of Canada in administrative and constitutional contexts, offers a principled basis upon which these questions may be answered defensibly and in a manner that better accords with Dworkin's interpretive theory of adjudication.

I. COMPUTERS, PRIVACY & THE LAW IN CONTEXT

Before evaluating the integrity of the law on search and seizure as it relates to computers, it would be prudent to briefly describe what “computers” includes and explain how these devices interact with the jurisprudence on section 8 of the *Charter*. Throughout this essay, the terms *computer*, *cell phone*, *smartphone*, *desktop*, *laptop*, *tablet*, *digital device*, and *electronic device* are used interchangeably. This is consistent with the way that those terms have been treated in section 8 jurisprudence. Although some have suggested that the law should distinguish between so-called “smart” and “dumb” technologies according to each device's individual capacities and functions, courts have repeatedly resisted attempts to distinguish between different phones, laptops, or computers.¹⁷ Section 8 of the *Charter* guarantees “the right to be secure against unreasonable search or seizure.”¹⁸ Since 1982, courts have developed a two-stage framework for analysis in order to answer if the right has been violated. First, does the claimant have a reasonable expectation of privacy in the subject matter of the search? If so, was the search reasonable?¹⁹ The latter question is the chief focus of this paper.

A. The Privacy Interests in Digital Information Are Unique

Before the Supreme Court of Canada's judgment in *R v Fearon*, a case affirming the reasonableness of searching a cell phone incident to arrest within circumscribed limits, there had been two conflicting currents among lower courts. The first of these schools held that the privacy interests engaged by a search of the informational contents of a cell phone are not significantly different than the interests in a diary, briefcase, or other physical document, each of which is ordinarily subject to being searched incident to arrest.²⁰ The second school ruled that an individual's privacy interests in the contents of his or her cell phone are qualitatively and quantitatively unique, attracting a heightened standard of protection, sometimes in the form of a warrant.²¹ Indeed, modern cell phones are essentially mini-computers capable of storing vast amounts of personal information, akin to little “Mary Poppins technologies” in which one can put as much data as she wants without them getting any heavier.²² With the speed of technological development, even the “dumbest” computer today has many times more memory and processing capacity than most desktop computers had 20 years ago, and there is nothing to suggest that this trend is slowing.

Any doubt that Canadian law does not or should not attribute a heightened privacy interest to such devices was resolved by the unanimous judgment in *R v Vu*²³ and affirmed in *Fearon*. As Justice Cromwell, writing for the majority, observed:

17 *R v Vu*, 2013 SCC 60 at para 38, [2013] 3 SCR 657 [*Vu*]; *Fearon*, *supra* note 9 at paras 51–54.

18 *Charter*, *supra* note 6, s 8.

19 Mathew Johnson, “Privacy in the Balance – Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8” (2012) 58 *Crim LQ* 442 at 475–476. See Part I.B, below, for a discussion of section 8's reasonableness requirements.

20 See e.g. *R v Giles*, 2007 BCSC 1147 at para 63, 77 WCB (2d) 469.

21 See e.g. *R v Hiscoe*, 2013 NSCA 48 at para 76, 328 NSR (2d) 381; *R v Polius*, [2009] OJ No 3074 at para 57, 196 CRR (2d) 288 (Ont Sup Ct) [*Polius*].

22 Amber Case, “We Are All Cyborgs Now” (December 2010), online: TED <http://www.ted.com/talks/amber_case_we_are_all_cyborgs_now/transcript> archived at <<https://perma.cc/7QJW-LVWW>>.

23 *Vu*, *supra* note 17 at paras 39–45, 47.

It is well settled that the search of cell phones, like the search of computers, implicates important privacy interests which are different in both nature and extent from the search of other “places”.... It is unrealistic to equate a cell phone with a briefcase or document found in someone’s possession at the time of arrest. As outlined in *Vu*, 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 thinks that it has been destroyed, and may provide access to information [stored on remote servers] that is in no meaningful sense “at” the location of the search...²⁴

Thus, subject to abandonment,²⁵ the idea that an individual has a reasonable expectation of privacy in the contents of his cell phone and other digital devices is no longer the subject of serious legal debate. Arguably beginning with the Supreme Court’s 2010 decision in *R v Morelli*²⁶ and culminating with *Fearon*, Canada’s treatment of electronic devices is a story of increasing recognition of the unique privacy interests that their information attracts. In particular, courts emphasize the values that privacy is thought to promote:

In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would *include* information which tends to reveal *intimate details of the lifestyle and personal choices of the individual*.²⁷

Much of the information stored on modern computers and smartphones falls into this “biographical core” of information that reasonable individuals in a democracy would expect to keep private. Significantly, however, not all information on a device must fall within this core in order to attract the *Charter*’s privacy protection. The question, in every case, as to whether an individual has a reasonable expectation of privacy in the subject matter of a search depends on the totality of the circumstances.²⁸ Since section 8 of the *Charter* protects against *unreasonable* searches by the state, one must have a reasonable expectation of privacy before an infringement can be found. This is not a particularly high threshold, since a finding that one has no reasonable expectation of privacy in any given context would effectively mean that there are no limits on the state’s ability to search.²⁹ Hence, in all but the exceptional case, electronic devices will attract a reasonable expectation of privacy sufficient to trigger the *Charter*’s protections.

B. Assessing the Reasonableness of Searching Digital Information

The law’s treatment of electronic devices is less consistent at section 8’s second stage of analysis. Whether the state’s interference with an individual’s reasonable expectation of privacy in the contents of his smartphone, computer, or other device is constitutional or not depends on a separate assessment of reasonableness. In *R v Collins*, the Supreme Court distilled this test into three requirements: the search must be authorized by law, the law itself must be reasonable, and the search must be conducted in a reasonable

²⁴ *Fearon*, *supra* note 9 at para 51.

²⁵ See e.g. *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579 where the accused was held to have abandoned any reasonable expectation of privacy in the contents of garbage bags placed at the edge of his property.

²⁶ *R v Morelli*, 2010 SCC 8, [2010] 1 SCR 253 [*Morelli*]. This case is discussed below in Part II.B.

²⁷ *R v Tessling*, 2004 SCC 67 at para 25, [2004] SCR 432 [*Tessling*, emphasis in original].

²⁸ Coughlan, *supra* note 8 at 99.

²⁹ *Ibid* at 87.

manner.³⁰ In *Hunter et al v Southam Inc* (“*Hunter*”), Justice Dickson (as he then was) held that an unwarranted search is *prima facie* unreasonable because the purpose of section 8 is to *prevent* unjustifiable intrusions into individual privacy, which could be guaranteed only by a system of prior judicial authorization based on reasonable and probable grounds where feasible.³¹ Indeed, in light of section 24(2)’s limited power to exclude unconstitutionally obtained evidence under the modern *Grant* test,³² the goal of *prevention* is all the more important.

Despite the Supreme Court’s strong, principled statements on section 8 early in the life of the *Charter*, within two decades some scholars were already lamenting the perceived decline in its privacy-protective potential.³³ This is nowhere more evident than in the checkered protection afforded to the high privacy interests in the informational contents of computers. The reasonableness of searching these devices currently varies greatly by context. For example, computers ordinarily require specific pre-authorization. In *R v Vu*, the Supreme Court held that when police find computers or cell phones in a dwelling, they are limited to seizing the devices and may not search them without obtaining a separate warrant under section 487 of the *Criminal Code*.³⁴ Only if the original search warrant explicitly contemplated the possibility that electronic devices would be found at the dwelling (and accordingly balanced these unique interests against the state’s interest in law enforcement) could police forego the specific warrant requirement.³⁵

By contrast, the requirement for specific pre-authorization is waived when the electronic device is searched incident to arrest within certain constitutional limits. Search incident to arrest is a common law doctrine that authorizes warrantless pat-down searches of an arrested person and things in his immediate vicinity.³⁶ A majority of the Court in *Fearon* extended the doctrine to allow police to examine the digital contents of any electronic devices the arrestee may be carrying, concluding that the investigative necessity of conducting quick, cursory searches in the context of an arrest was sufficiently important to outweigh the individual’s interest in privacy.³⁷ However, this does not mean police are free to search any device or its entire contents incident to arrest. The arrest must be lawful; the search must be truly incidental to arrest in that it is conducted for a valid common law purpose such as to protect the public, preserve evidence from destruction, or discover evidence relevant to the offence for which the individual has been arrested; and the search must be conducted in a reasonable manner. Furthermore, the nature and extent of the search should be tailored to the purpose for the search and police must take detailed notes throughout.³⁸

30 *R v Collins*, [1987] 1 SCR 265 at para 23, 56 CR (3d) 193 [*Collins*].

31 *Hunter et al v Southam Inc*, [1984] 2 SCR 145 at 160–162, 55 AR 291 [*Hunter*]. The decision need not be made by an actual judge, but by a body “capable of acting judicially.”

32 Absent bad faith on the part of the police, oftentimes *not* admitting the evidence would tend to bring the administration of justice into disrepute. See *Grant*, *supra* note 14 for the complete test and a list of considerations.

33 See e.g. Don Stuart, “The Unfortunate Dilution of Section 8 Protection: Some Teeth Remain” (1999) 25 *Queen’s LJ* 65.

34 *Criminal Code*, RSC 1985, c C-46, s 487 [*Code*].

35 *Vu*, *supra* note 17 at para 2.

36 *R v Caslake*, [1998] 1 SCR 51 at para 13, 123 Man R (2d) 208 [*Caslake*].

37 *Fearon*, *supra* note 9 at para 49. Contrast the Supreme Court of Canada’s approach with the Supreme Court of the United States’ unanimous decision in *Riley v California*, 573 US ____ (2014) [*Riley*]. There, the Court held that the search incident to arrest doctrine in the United States does *not* generally authorize police to search a cell phone’s data without a warrant, owing in part to the qualitative and quantitative differences between cell phones and non-digital containers.

38 *Fearon*, *supra* note 9 at para 83.

Different still is the way electronic devices are treated at the Canadian border. Most travellers are accustomed to having border officials look through their luggage, or they are at least aware customs officers have this power. What people do not realize is just how extensive those powers are. The *Customs Act* requires all persons arriving in Canada to present themselves to customs officials, to answer all questions truthfully, and to report all goods a passenger is importing, including any goods that originated in Canada and are being brought back.³⁹ Section 99(1)(a) of the *Act*'s enforcement provisions empower officers to "examine any goods that have been imported and open or cause to be opened any package or container of imported goods and take samples of imported goods in reasonable amounts."⁴⁰ Section 101 allows customs officials to detain goods until they have been dealt with according to the statute.⁴¹ Meanwhile, a "good" is defined broadly as including "conveyances, animals and any document in any form."⁴² Most importantly, the general power in section 99(1)(a) is distinguishable from other provisions in the statute in that it does not require reasonable grounds to suspect a contravention—that is, individualized reasonable suspicion—before an agent may search the good.⁴³ In fact, no grounds whatsoever are required before an agent can conduct an allegedly routine or random search of a traveller's goods. Lower courts in Ontario have upheld the constitutionality of this broad and general statutory power as a result of the combined effect of sections 99(1)(a) and 101.⁴⁴

In the 1988 case of *R v Simmons*, the Supreme Court considered whether former provisions authorizing a strip search under the *Customs Act* were reasonable and thus constitutional within the meaning of section 8 of the *Charter*. These provisions were substantially similar to section 98 of the modern *Act*, which regulates personal searches. Although the search in that case was not conducted in a reasonable manner and therefore fell on the third branch of *Collins*' reasonableness criteria, the majority held that the provisions authorizing the search were reasonable in spite of the fact that they did not conform to the default requirement of pre-authorization on reasonable and probable grounds set out in *Hunter*. At the border, the lesser requirement of reasonable suspicion combined with a statutory right of secondary authorization by a supervisor was not unreasonable.⁴⁵ The Court's consensus was that the border places individuals in a unique position in which they have a lowered expectation of privacy and the state has a strong interest in sovereign self-protection.⁴⁶ Chief Justice Dickson then delineated three categories of border searches according to their intrusiveness and the degree of protection they require: (1) routine questioning, searches of baggage, or "frisks" to which most travellers are subjected and which attract no stigma or constitutional issues; (2) strip searches in a private room like the one in *Simmons*; and (3) body cavity searches, which are to be considered highly invasive of privacy and deserving of stronger protection.⁴⁷

39 *Customs Act*, *supra* note 1, ss 11(1), 12(1), 12(3.1), 13.

40 *Ibid*, s 99(1)(a).

41 *Ibid*, s 101.

42 *Ibid*, s 2.

43 See e.g. *ibid*, s 98, according to which a search of the person requires reasonable grounds to suspect "that the person has secreted on or about his person" anything that contravenes the *Customs Act*, would afford evidence of a contravention, or which is prohibited or controlled from importation. For greater certainty that individualized suspicion is not a requirement for conducting a "non-intrusive examination" of goods, see also s 99.3.

44 *R v Agyeman-Anane*, [2009] OJ No 6005 at paras 33–35, 2009 CarswellOnt 5956 (Ont Sup Ct); *R v Corbyn*, [2005] OJ No 5578 at para 68, 2005 CarswellOnt 8299 (Ont Sup Ct).

45 *Simmons*, *supra* note 16 at paras 42, 50–51.

46 *Ibid* at paras 24, 48.

47 *Ibid* at paras 27–28.

It is worth pausing to consider Chief Justice Dickson's statement that "no constitutional issues are raised" by the first category of border search. This does not mean that one has *no* reasonable expectation of privacy in his or her baggage and cannot cross the threshold to trigger constitutional protection. It means only that one's expectation of privacy is presumptively *lower* at the border than in other contexts,⁴⁸ which is no bar to section 8's guarantee. *Simmons* stands for the proposition that if the search is of the first routine type, then the search is rendered reasonable, and thus constitutional, *by virtue of the fact that it occurs at the border*. Ostensibly, a computer and other electronic devices are "goods" within the ambit of the *Customs Act's* broad definition. It would be foolish to suggest otherwise, and no court has tried. In the rare cases where an individual has challenged a border search as unreasonable post-*Simmons*, courts have consistently found that computers and cell phones are "goods" and are subject to routine searches of their contents like any other pocket, bag, or container.⁴⁹ This statutory interpretation, coupled with border officers' broad powers under the *Act* and Chief Justice Dickson's ruling in *Simmons*, means that customs law currently authorizes searches of electronic device contents without a warrant, without reasonable suspicion, and without any discernible limits.

The reasonableness of searching these devices that attract high privacy interests has depended greatly on the context and countervailing state interests that arise at the location of the search. To search a computer at home, police need a specific warrant. To search a computer incident to arrest, police do not need a warrant, but must have had grounds for the arrest pursuant to which the search is conducted. To search a computer at the border, officers require no grounds at all. Notwithstanding the unique situations that have been used to justify treating these devices differently in different contexts, this situational interpretation of section 8's reasonableness requirement does not fit or justify an undeniable trend in the jurisprudence towards *greater* recognition of and *more* protection for the heightened privacy interests that people hold in their devices. Thus, Dworkin's theory of law as integrity suggests that these situational contexts cannot single-handedly justify the vastly differential treatment of electronic devices in the face of their distinctive privacy interests.

II. SEARCHING ELECTRONIC DEVICES INCIDENT TO ARREST

In December 2014, the Supreme Court of Canada affirmed a decision of the Ontario Court of Appeal permitting police to search cell phones and similar devices incident to arrest without a warrant. Privacy advocates have described the ruling in that case, *R v Fearon*, as a "major disappointment."⁵⁰ While this assessment stems from a normative, pro-privacy rights perspective, *Fearon* is equally disappointing from the vantage point of law as integrity. The majority opinion written by Justice Cromwell is unlikely to be just because it does not exhibit the coherence that law as integrity requires. His interpretation as to the reasonableness of searching cell phones incident to arrest is incoherent because it allows a descriptive interpretation to obfuscate the normative nature of privacy under the *Charter*, it fails to account for the original justification for the search incident to arrest doctrine, and it imposes arbitrary search protocols that protect neither the individual's nor the state's interests. In this way, Justice Cromwell's constructive interpretation of the law does not strike a truly proportional balance between privacy and law enforcement, despite his intention to do just that.

48 *Ibid* at para 49.

49 *R v Leask*, 2008 ONCJ 25 at para 16, 167 CRR (2d) 267 [*Leask*]; *R v Saikaley*, 2012 ONSC 6794 at paras 79–82, [2012] OJ No 6024 (QL); *Buss*, *supra* note 5 at para 25.

50 Kassie Seaby & Raji Mangat, "Making Privacy Meaningful in a Digital Age" (15 December 2014), *British Columbia Civil Liberties Association* (blog), online: <<http://www.bccla.org/2014/12/making-privacy-meaningful-in-a-digital-age>> archived at <<https://perma.cc/8VPG-J4EC>>.

A. Law as Integrity

Before appreciating the ways in which the majority's judgment does not fit or justify the law of searching electronic devices under section 8 as a whole, one must grasp the interpretive theory of adjudication that serves as a basis for the analysis. In *Law's Empire*, Ronald Dworkin argues that each case offers its own constructive interpretation of the law that shows the law as a whole in its best light, as though a single author wrote the entire body of law.⁵¹ Ironically, a single author did, in fact, write the leading judgments in *R v Vu* and *R v Fearon*.⁵² It is therefore especially troubling that the common law rules generated by the former decision stand in such sharp contrast to those produced by the latter. As briefly discussed above, Dworkin's virtue of integrity contends that while individuals in a pluralistic society may disagree about the particular ends of justice, society can be assured that judges act justly when they act coherently, as to act capriciously is to act without integrity, and by caprice one will only achieve justice by accident.⁵³ A commitment to integrity signifies that what courts have done in the past is relevant to what they ought to do in the present instance. It requires courts to actively engage with their past decisions. This does not necessarily mean courts must repeat every historical *ratio decidendi*: following, overruling, or distinguishing a case are all ways courts may demonstrate integrity.⁵⁴ Silence, on the other hand, will not count. Justice Cromwell's reasons in *Fearon* do not engage with significant aspects of the legal text which, had they been addressed, might have led to a different and more just result.

To be clear, this is not to suggest that there is an objectively discernible, "correct" story latent in the text, divorced from the individual convictions of the interpreter as to how the story can be made the best it can be. According to Dworkin, this would be a misleading objection.⁵⁵ However, fit and justification serve as measures by which constructive interpretations may be judged as more or less correct *as a matter of interpretative practice*. It is therefore possible to subject Justice Cromwell's opinion to the tests of fit and justification posited, if imperfectly, by a theory of law as integrity. Admittedly, this analysis is limited to the extent that it is not possible to neatly discriminate between the rigours required by fit as opposed to justification. Dworkin describes these two dimensions as interrelated and complex.⁵⁶ They necessarily require "a delicate balance among...political convictions of different sorts."⁵⁷ He downplays the significance of the distinction because in most cases one interpretation may fit more of the text than another,⁵⁸ which could be determinative. Still, the assessment as to what will and will not count as "fitting" the legal text is itself a political decision.⁵⁹ Thus, for Dworkin there is no real separation between law and morality.⁶⁰

Still, the regulative power of law as integrity is hardly devoid of any practical application. On the contrary, the difference between fit and justification can be understood to roughly parallel legal and political decision-making as part of an interpretive exercise. "Fit" is used as a threshold test to judge competing interpretations as eligible and ineligible solely

51 Dworkin, *supra* note 10 at 225–226.

52 I assume for the sake of argument that to the extent court judgments might have been substantially drafted by a law clerk or someone other than the judge, the judge's choice to sign the opinion effectively underwrites the integrity of the decision (or lack thereof, as the case may be).

53 See Introduction, "Method", above.

54 Hershovitz, *supra* note 12 at 116–117.

55 Dworkin, *supra* note 10 at 238.

56 *Ibid* at 231, 239.

57 *Ibid* at 239.

58 *Ibid* at 231.

59 *Ibid* at 257.

60 Arthur Ripstein, ed, *Ronald Dworkin* (New York: Cambridge UP, 2007) at 14.

by reference to the legal text.⁶¹ “Justification” need only arise when there are two or more eligible interpretations. It asks which of the interpretations is most defensible in that it shows the law in its best light.⁶² Again, this is an oversimplification because whereas one judge may deem an interpretation eligible, another might rule that interpretation ineligible. Thus, where the judge sets his threshold for “fit” is itself subject to justification. By the same token, just because one interpretation provides a *better* fit than any other does not automatically rule out the other interpretations if they can be said to meet the threshold for fit and are justified by principles of justice and fairness that, if accepted by the community, would show the law in its best light.

Despite this interpretive ambiguity, Dworkin clearly states that it would demonstrate bad faith if a judge determined an interpretation’s fit according to a normative standard outside the text.⁶³ He also suggests the best constructive interpretation will have general explanatory power without leaving any “major structural aspect of the text” unexplained.⁶⁴ What will or will not count as a major, as opposed to a minor, structural aspect is unclear from Dworkin’s writing; however, if the justification advanced by the court for its interpretation directly contradicts existing precedent without explicitly distinguishing those parts of the text, then it may expose not only gaps in justification, but also fissures in fit.

Dworkin is not without his critics. For example, legal philosopher Joseph Raz rejects any theory of law that requires judges to decide cases as though courts speak with one voice. This, he says, diminishes the inescapably political character of judicial decision-making.⁶⁵ According to Raz, the flaw in law as integrity is that it presumes the existence of an “inner legal logic which is separate from ordinary moral and political considerations of the kind that govern normal government, in all its branches.”⁶⁶ In other words, it is false to presume that there is ever a single right answer, even if Dworkin’s measures of fit and justification suggest that there is. Raz argues that the risk with construing Dworkin’s integrity as requiring strong coherence with past decisions is that it gives undue weight to fit and not enough to justification based on moral value.⁶⁷ Although Dworkin does not provide a mechanism for resolving these conflicts, it is precisely because there is rarely a consensus as to the moral value of one decision versus another that fit is a desirable baseline for courts to consider as they make decisions on what the law is or what it should be. There may be more than one just outcome in cases like *Fearon* or Philippon’s, but insofar as courts are held accountable through their reasons and they strive to follow or distinguish precedent, some interpretations are clearly better than others.

B. A Poor Constructive Interpretation

According to law as integrity, Justice Cromwell’s judgment in *Fearon* must be understood as a constructive interpretation of the law as a whole and as it relates to the reasonableness of searching electronic device contents. His interpretation does not fit with several fundamental principles in this area of the law. As such, despite appearances, *Fearon* does not represent a “hard case” in which one had to choose between multiple eligible interpretations. If the Supreme Court had demonstrated the engagement with these seemingly neglected aspects of the chain novel as required by integrity, then it is

61 Dworkin, *supra* note 10 at 255.

62 *Ibid* at 231.

63 *Ibid* at 255.

64 *Ibid* at 230.

65 Joseph Raz, “Speaking with One Voice: Dworkinian Integrity and Coherence” in Justine Burley, ed, *Dworkin and His Critics: With Replies by Dworkin* (Oxford: Blackwell Publishing, 2004) 285 at 285.

66 *Ibid* at 289.

67 *Ibid* at 288.

unlikely the majority would have reached the same decision. Firstly, Justice Cromwell does not acknowledge the normative roots of privacy under the *Charter*. For instance, in *R v Tessling*, the Supreme Court unanimously held that privacy is a normative rather than a descriptive standard.⁶⁸ In other words, one should not lose *Charter* protection simply because he or she expects that someone is spying.⁶⁹ Although the court in *Tessling* discussed privacy in terms of the threshold question—whether or not one has a reasonable expectation of privacy in the first place and is thus entitled to *Charter* protection at all—if privacy is normative at that stage of analysis, one cannot ignore its normative influence at the second stage when the court must assess whether a search was reasonable. This reasonableness assessment necessarily involves a balancing of the state and individual interests at play, which requires judges to characterize the level or significance of the individual’s privacy interest.⁷⁰ In *Fearon*, Justice Cromwell characterized the intrusion into the contents of the accused’s phone as follows:

[I]n marked contrast to...bodily sample seizures [which always require a warrant]...while cell phone searches have the potential to be a significant invasion of privacy, they are neither *inevitably* a major invasion of privacy nor *inherently* degrading. Looking at a few recent text messages or a couple of recent pictures is hardly a massive invasion of privacy, let alone an affront to human dignity.⁷¹

The problem with this comparison is that it cites the specific facts in *Fearon*, in which only a photo of a handgun and an incriminating draft text message were subjects of the initial search, as proof that searches of electronic devices are not inherently intrusive. This is a purely descriptive account of the physical intrusiveness of such a search in *one* case that does not account for the individual’s subjective experience of the intrusion, nor society’s collective interest in characterizing the interest as particularly significant. To account for the normative understanding of privacy that the Supreme Court had previously endorsed, Justice Cromwell ought to have asked not whether the contents of electronic devices differ markedly from bodily samples, but whether this is the kind of privacy interest that the law *should* regard highly in a free and democratic society, notwithstanding its similarity or dissimilarity to non-electronic vessels of information.

Although this effectively judges the “fit” of Justice Cromwell’s reasonableness interpretation according to a normative standard, this observation does not run afoul of Dworkin’s law as integrity. While it is disingenuous to judge fit according to a normative standard, an important distinction must be drawn in the present context. Here, the normative standard is not one that I have chosen as morally right; rather, privacy’s normative character *is the law* against which any constructive interpretation must fit. In this way, the interpretation advanced in *Fearon* does not cohere with *the law’s* understanding of privacy. In fact, it is telling that Justice Cromwell never refers to the Supreme Court’s earlier decision in *Tessling*, whereas Justice Karakatsanis does in her dissenting opinion. Therefore, he does not meaningfully engage with the normative aspect of privacy, contrary to the requirements of law as integrity.

Justice Cromwell’s descriptive account of the informational privacy interest is also silent on the Court’s previous characterization of a computer search’s intrusiveness. In *R v Morelli*, a child pornography case in which there were insufficient grounds to issue a search warrant, a majority of the Court characterized the privacy interest as follows:

68 *Tessling*, *supra* note 27 at para 42.

69 *R v Wong*, [1990] 3 SCR 36 at 51, 60 CCC (3d) 460.

70 Coughlan, *supra* note 8 at 91–92.

71 *Fearon*, *supra* note 9 at para 61 [emphasis in original].

...it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer. Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.⁷²

Although the computer in *Morelli* was found in the accused's home, the majority's statement is no less true of portable electronic devices. It is precisely because cell phones are portable that the privacy interest in them should be so high. The fact that cell phones are carried on one's person make them, quite literally, the most personal computers in use today. This characterization of the intrusiveness of a computer search as being the most invasive of privacy and most revealing of sensitive information—more than a strip search or a body cavity search—bumps up against Justice Cromwell's notion that cell phone searches are not inherently problematic. One would have to strain to see how the interpretation of the law offered by *Fearon* could be interpreted as having been written by the same author as *Morelli*, barring a split personality disorder. These two interpretations are incoherent, raising questions as to whether the Court was acting morally then, now, or not at all.

Secondly, the majority's interpretation of the reasonableness of permitting cell phone searches incident to arrest leaves a major structural aspect of the legal text unexplained. One of Justice Cromwell's principal justifications for allowing electronic devices to be searched incident to arrest is that individuals have a reduced expectation of privacy after arrest.⁷³ If the objective of a judge who acts with integrity is to make the law "the best it can be," then this justification falls short because it too does not fit, nor does it explain, what came before. For example, since section 8 of the *Charter* necessarily involves an evaluation as to whether the state's interest is superior to that of the individual's in a given situation, a warrant requirement was originally preferred to determine *if* the state's interest prevailed on a case-by-case basis. By contrast, the doctrine of search incident to arrest was originally premised on an assumption that the state's interest in protecting the police and in preserving evidence after an arrest will *always* trump any legitimate expectation that the arrestee may have. In *R v Caslake*, the Supreme Court stated:

The authority for the search [incident to arrest] does *not* arise as a result of a reduced expectation of privacy of the arrested individual. Rather, it arises out of a need for the law enforcement authorities to gain control of things or information *which outweighs the individual's interest in privacy*.⁷⁴

According to this logic, imposing a warrant requirement to weigh these competing interests after arrest would be redundant.⁷⁵ However, while this assumption might have been true when the Court released *Caslake* in 1998, it does not fit with the Court's subsequent recognition of the heightened and different privacy interests engaged by the contents of electronic devices. It is a simple fact of history that in 1998 cell phones were still relatively novel and unsophisticated. Today, they are ubiquitous and intelligent.

In this new context, the state's overwhelming interest in intruding upon the individual's privacy after arrest cannot be automatically presumed. In *Vu*, Justice Cromwell suggested that the basis for normally requiring a separate, specific warrant for computers is that one cannot reasonably infer or assume that the justice who issued the original warrant took account of the unique privacy interests that would be affected if the search extended to

72 *Morelli*, *supra* note 26 at para 105.

73 *Fearon*, *supra* note 9 at para 56.

74 *Caslake*, *supra* note 36 at para 17 [emphasis added]. See also Coughlan, *supra* note 8 at 92.

75 *Polius*, *supra* note 21 at para 47.

the informational contents of computers discovered in that place.⁷⁶ By the same token, one cannot take for granted that the constitutional justification for waiving the warrant requirement for searches incident to arrest (i.e. that the state's interest after an arrest is so great as to override any privacy interest the arrestee may have) is equally true in the context of a device whose informational contents engage a range of very high privacy interests, a finding that Justice Cromwell himself endorsed. To be fair, Justice Cromwell acknowledges that there is a potential for greater privacy intrusions when police search the contents of cell phones incident to arrest, which is why he adds the requirement that police take detailed notes of their search of any electronic device to aid after-the-fact judicial review.⁷⁷ So, he does not necessarily assume that the interest balancing after an arrest inevitably favours the state; however, his greater problem from a perspective of law as integrity is that the justification he *does* offer for allowing cell phone searches incident to arrest—that arrested individuals have a reduced expectation of privacy—directly contradicts the essential premise on which the search incident to arrest doctrine was founded. It is true that a valid constructive interpretation need not fit every aspect of the text to be eligible and history is only relevant to integrity insofar as it facilitates consistency of principle in modern practice;⁷⁸ yet, a principle as crucial as this, even if historic, cannot be ignored. To the extent that this original justification no longer fits with contemporary principles of justice, then integrity required that the Court at the very least explain why its new justification is to be preferred over the other and how this, too, fits with the doctrine of search incident to arrest in every other context where police are *not* required to take detailed notes. Unfortunately, the decision does not engage with the ontological claim in *Caslake*, quoted above, and therefore does not demonstrate the fit demanded by law as integrity.

Lastly, Justice Cromwell's constructive interpretation of the reasonableness of searching cell phones incident to arrest imposes "search protocols" like those he specifically criticized as counterproductive in *Vu*. The Supreme Court has repeatedly affirmed, beginning in *Hunter*, that the purpose of section 8 is to *prevent* unreasonable searches *before* they occur, giving rise to the presumptive warrant requirement.⁷⁹ Justice Cromwell never expressly invokes or acknowledges this purpose of section 8 in *Fearon*. However, his project can be broadly interpreted as endeavouring to prevent unreasonable searches of cell phones incident to arrest from occurring, not by requiring prior authorization to balance state and privacy interests, but by balancing those interests in advance and circumscribing the limits within which an unwarranted search of such devices will be permissible.⁸⁰ In particular, *Fearon* permits a cursory search of a digital device's contents, limiting which computer applications police will generally be able to access and requiring law enforcement officials to take detailed notes on what they searched and how.⁸¹ This does not fit with Justice Cromwell's earlier comments on the futility of such search protocols. Indeed, he held in *Vu* that it is not always possible or desirable to restrict police access to certain parts of a device based on assumptions about where evidence is likely to be stored. Such search protocols can be misguided and deprive police of access to well-hidden, yet highly relevant evidence.⁸² Again, to be fair, Justice Cromwell restricts his reasons in that case to situations where a warrant must be obtained, regarding search protocols on top of a warrant to be an undue burden.⁸³ However, his decision in *Fearon* does not take up these qualms.

76 *Vu*, *supra* note 17 at para 2.

77 *Fearon*, *supra* note 9 at paras 63, 82.

78 Dworkin, *supra* note 10 at 227, 230.

79 *Hunter*, *supra* note 31 at para 27; *R v Dyment*, [1988] SCR 417 at para 23, 55 DLR (4th) 503.

80 See *Fearon*, *supra* note 9 at para 82 for a checklist of these requirements.

81 *Ibid* at paras 76–77, 82.

82 *Vu*, *supra* note 17 at paras 57–59.

83 *Ibid* at paras 59, 63.

One can infer from his reasons that the Court justifies the incoherence on the basis that police have an investigative need to search these devices promptly after an arrest.⁸⁴ Ultimately, however, an interpretation that accounts for *both* these pragmatic concerns and legal conventions, consistent with Dworkin’s law as integrity, would privilege prior authorization of such devices. For instance, if police proceed to conduct a cursory search of a cell phone incident to arrest and it yields no evidence in the places they would have *expected* to find some, then even if the search complied with Justice Cromwell’s standards of “reasonableness” in *Fearon*, it would be difficult for the police to then argue that they still had reasonable grounds to believe the phone contained evidence. The net result is that this type of pre-emptive search, which Justice Cromwell interpreted as fitting and justifying the law as a whole, might actually impair the police’s ability to obtain a warrant, even as evidence is hidden in another area of the device. This interpretation advances neither the state’s interest in law enforcement, nor the individual’s interest in privacy. In this way, a constructive interpretation of the law on searching electronic devices that does not in any defensible way account for the cogent reasons for rejecting computer search protocols undermines the law’s integrity.

To be clear, I am not suggesting that Justice Cromwell is not a person of integrity generally, or that he does not strive to act morally and with integrity when he writes legal opinions. Indeed, the mere fact that he or any judge cites precedent to support his decisions by itself demonstrates, at the very least, an aspiration to act with integrity.⁸⁵ However, when one seeks to act with integrity, he should then be meticulous in doing so, as it opens him up to criticism that his interpretation of the law leaves significant aspects of the record unexplained. That is what happened here. The majority opinion in *Fearon* deemed eligible a constructive interpretation that neither fits nor justifies the law as a whole because it fails to fully engage with the normative roots of privacy, to consider the primordial justification for the doctrine of search incident to arrest, and to explain why search protocols are any less futile or any more proportional than requiring a warrant or independent reasonable grounds for the search. Therefore, a better interpretation is needed.

III. SEARCHING ELECTRONIC DEVICES AT THE BORDER

On its face, *Fearon* appears to dial back the privacy gains made in cases like *Vu*. If one accepts that the majority’s decision in *Fearon* does not fit or justify the law on searching electronic devices as a whole—a law that clearly affirms the heightened and different privacy interests engaged by the contents of personal electronic devices compared to traditional receptacles—then a better constructive interpretation should be offered that may guide the law’s development at the border. The law may be shown in its best light when the reasonableness of searching an electronic device focuses on the proportionality between the limits on privacy and the benefit to be gained as a result. Proportionality in section 8 ought to mimic the way proportionality has developed under section 1 of the *Charter* and in judicial review of discretionary administrative decisions affecting *Charter* protections. A proportional balance according to this interpretation would demand—at a minimum—a requirement for reasonable suspicion before an electronic device could be searched at the border.

84 *Fearon*, *supra* note 9 at paras 49, 59, 66. Justice Cromwell also points to the restrictions imposed on strip searches conducted incident to arrest as evidence that an appropriate balance may be struck at para 62. Contrast this conclusion with Chief Justice John Roberts’ opinion in *Riley*, *supra* note 37 at 13–14, that concerns about the destruction or “remote wiping” of evidence triggered by an arrest are “anecdotal.” The Court held that, in most cases, cell phones will automatically lock such that an officer’s opportunity to search digital information incidental to arrest will be practically limited and, furthermore, officers could preserve digital evidence by simply disconnecting a phone from its cellular network until they obtain a warrant.

85 Hershovitz, *supra* note 12 at 118.

A. Distinguishing *R v Fearon*

Integrity requires that future cases on computer searches engage with the choices made in *Fearon*, but it does not condemn judges to agree with them. For instance, the notion that *stare decisis* should compel judges to apply decisions they have come to realize are wrong does not fit or justify legal practice.⁸⁶ This is what Dworkin means when he says that law as integrity begins in the present.⁸⁷ His theory asks how one can justify what lawmakers have done in an overall story worth telling *today*. This means integrity may require judges to overrule a bad decision in order to make the law the best that it can be.

For instance, in *Carter v Canada*, the Supreme Court ruled that the prohibition on physician-assisted suicide was unconstitutional even though it had reached the opposite conclusion 22 years earlier.⁸⁸ In making its decision, the Court had to consider whether the trial judge was bound by the Court's prior judgment in a case with substantially similar facts. A unanimous Bench held that she was not:

...*stare decisis* is not a straitjacket that condemns the law to stasis. Trial courts may reconsider settled rulings of higher courts in two situations: (1) where a new legal issue is raised; and (2) where there is a change in the circumstances or evidence that "fundamentally shifts the parameters of the debate"....⁸⁹

Note that the two situations listed by the Court are specifically limited to when *trial courts* may reconsider settled rulings of higher courts. *Carter* places no restriction on when the Supreme Court may reconsider its own decisions. It is thus clearly open to the Court to reconstitute the law in cases where neither a new legal issue is raised nor have circumstances changed, but where the Bench has come to realize that an alternative interpretation of the law better fits and justifies legal practice. The rub is that if lower courts cannot lawfully cast doubt on the Supreme Court's decisions, then the Supreme Court may be less likely to recognize or acknowledge the error of its ways.

If, as I have argued, the interpretation of the law put forth by Justice Cromwell in *Fearon* leaves major parts of the text unexplained, then that decision might not be just and cannot preclude the law's advancement in a different direction. *Fearon* has led some observers to believe that if it is reasonable for police to search one's smartphone incident to arrest without a warrant, then it is almost certainly reasonable for agents to search the same electronic devices without specific prior authorization at the Canadian border.⁹⁰ According to this logic, no constructive interpretation that limits searches of computers at the border would fit with the informational privacy U-turn that *Fearon* has added to the chain novel. However, this conclusion does not necessarily follow for two reasons. First, an eligible interpretation of the law need not fit every part of the text to demonstrate integrity, particularly if that part is deficient.⁹¹ Second, notwithstanding the Court's clear intent in *Simmons* to exempt routine border searches from the constitutional safeguards first articulated in *Hunter*, an important distinction should be made between the arrest and border contexts. Even accepting the outcome in *Fearon*, which at the very least affirmed the unique privacy interests engaged by cell phones even if it did not balance

86 *Ibid* at 103.

87 Dworkin, *supra* note 10 at 227.

88 *Carter v Canada (AG)*, 2015 SCC 5, [2015] 1 SCR 331 [*Carter*].

89 *Ibid* at para 44.

90 Mark Joseph Stern, "The Cops Can Pretty Much Always Search Your Smartphone in Canada" (6 March 2015), *Future Tense* (blog), online: <http://www.slate.com/blogs/future_tense/2015/03/06/alain_philippon_case_cops_can_search_your_cellphone_in_canada.html> archived at <<https://perma.cc/ST6P-Y8TS>>.

91 Dworkin, *supra* note 10 at 230.

those interests accordingly, a lawful search incident to arrest must be the result of a lawful arrest. A lawful arrest requires reasonable grounds to believe the individual has committed or is about to commit an offence.⁹² By contrast, the *Customs Act* does not require any grounds before a border agent is empowered to examine a traveller's goods, including any electronic devices.⁹³ As such, if no judge is willing to reverse *Fearon*, it may be distinguished without undermining the new constructive interpretation of the law that I propose on the basis that at least *some* consideration is afforded to the arrestee's heightened privacy interest in his devices in a search incident to arrest. By comparison, allowing unrestricted, indiscriminate searches of the same devices at the border when the *Charter* guarantees the right to be secure against unreasonable search and seizure appears, at least notionally, to be the antithesis of reasonableness. Therefore, distinguishing *Fearon* is not only consistent with, but also required by law as integrity. This case poses no meaningful threat to developing a more coherent interpretation of a computer search's reasonableness under section 8.

B. A Fourth Category?

That courts have repeatedly asserted the border is not a "*Charter-free zone*"⁹⁴ suggests that privacy does and should still matter when an individual seeks to enter the country. In 1988, when *Simmons* was decided, a computer was something that few people owned and no one could carry in his pocket. As such, one has to wonder whether Chief Justice Dickson might have recognized a fourth type of border search—that of computers—and assigned special protections to such devices just as *Vu* did in the warranted context. In *Simmons*, the Court held border strip searches (the second category) were reasonable under the *Customs Act*. However, Chief Justice Dickson emphasized that what made them reasonable was not the state's interest in national security by itself, but also the added requirement that the border officer reasonably suspect that the traveller was secreting something on or about her person and the availability of a statutory right to seek secondary authorization.⁹⁵ The need for these additional safeguards were essential to render a strip search reasonable due to the more intrusive nature of that type of search compared to a routine search of goods.

Given the law's recognition that computers are unique in both the nature and volume of information they contain, thereby attracting different privacy interests, it is unreasonable that they would be subjected to a search like any other good without individualized suspicion. Justice Nadel of the Ontario Court of Justice rejected this argument in *R v Leask*. The accused, a trucker, was charged with possession and importation of child pornography after customs officials discovered 33 illicit videos on a laptop in the cab of his vehicle. Justice Nadel held that searching a computer without any special equipment was no more intrusive or embarrassing than searching a pocket or a purse, which is permitted without reasonable suspicion.⁹⁶ The problem with this stance is it uses the same misleading digital-analogue comparisons that delayed legal recognition of a computer's *unique* privacy interests in order to now deny the greater intrusiveness of interfering with them. This is an untenable conclusion that breeds incoherence and skepticism in the law, which fails to fit or justify the law as a whole.

Even if one were to assume that searching a computer is not *as intrusive* as a strip search—and Justice Fish's comments in *Morelli* certainly challenge such an assumption—this would not justify lumping computers together with all other goods at the border. For

92 *Code*, *supra* note 34, s 495.

93 *Customs Act*, *supra* note 1, s 99(1)(a).

94 *Buss*, *supra* note 5 at para 35.

95 *Simmons*, *supra* note 16 at para 51.

96 *Leask*, *supra* note 49 at para 16.

example, a 2014 study on Americans' attitudes toward a series of traditional and electronic border searches found that content-related searches of electronic devices are perceived to be "among the most intrusive [...], the *most* revealing of sensitive information, [and] only less embarrassing than strip searches and body cavity searches..."⁹⁷ Attitudes may vary slightly in Canada, adjusting for a more deferential political culture; however, there is no reason to suspect that a similar study among Canadians would yield vastly different results. Ergo, it is wrong to suggest, as Justice Nadel did in *Leask*, that a computer is a good like any other "in the context of the border."⁹⁸ The qualities of a computer that invite heightened privacy interests in the information it contains are not magically transformed when an individual seeks entry to Canada. The only things that arguably change are the nature and significance of the state's countervailing interests. Yet, under section 8, courts have traditionally assessed the balance of these interests with disproportional emphasis on the external situation in which the search occurs. While *Simmons* is regularly cited as evidence that computer searches absent individualized suspicion are reasonable because they fall within the first category of "routine" searches of goods, that decision should not be read apart from Chief Justice Dickson's caution:

It is true that a determination of reasonableness must depend to some degree on the circumstances in which a search is performed. In my view, however, it would be incorrect to place overwhelming emphasis on the surrounding circumstances when assessing reasonableness under s. 8. Regardless of the constraints inherent in the circumstances, the safeguards articulated in *Hunter v. Southam Inc.* should not be lightly rejected. Although *Hunter* did not purport to set down immutable preconditions for validity applicable to all searches, the Court arrived at the...minimum prior authorization requirements only after examining the values s. 8 is meant to protect. Foremost among these values is the interest in preventing unjustified searches before they occur. This is a basic value regardless of situational constraints. In light of the importance of preventing unjustified searches, departures from the *Hunter v. Southam Inc.* standards that will be considered reasonable will be exceedingly rare.⁹⁹

The fact that Chief Justice Dickson sought to craft categories of border searches requiring different levels of protections at all suggests it is unreasonable to continue to treat computers the same as any other goods at the border, unless one can demonstrate that the state's interest in national security *so outweighs* the individual's interest in privacy. According to proportionality theory, one cannot.

C. The Border Fallacy

What is it about borders in particular that would justify permitting content-related searches of electronic devices absent any reasonable grounds? Numerous rationales have been advanced, including self-defence, public health, and enforcement of tax and criminal offences. The Ontario Court of Appeal went so far as to recognize the need to protect the national border as a principle of fundamental justice.¹⁰⁰ In that case, *R v Jones*, the issue was whether the principle against self-incrimination prevented the accused's answers to routine questions by border agents from being used in criminal proceedings. In ruling the evidence admissible, the Court described the border context in the following terms:

97 Matthew B Kugler, "The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study" (2014) 81:3 U Chicago L Rev 1165 at 1196 [emphasis in original].

98 *Leask*, *supra* note 49 at para 14.

99 *Simmons*, *supra* note 16 at para 47.

100 *R v Jones* (2006), 81 OR (3d) 481 at para 31, 41 CR (6th) 84 (Ont CA) [*Jones*].

Travellers...reasonably expect that Customs authorities will routinely and randomly search their luggage. Put simply, the premise underlying the principle against self-incrimination, that is, that individuals are entitled to be left alone by the state absent cause being shown by the state, does not operate at the border. The opposite is true. The state is expected and required to interfere with the personal autonomy and privacy of persons seeking entry to Canada. Persons seeking entry are expected to submit to and co-operate with that state intrusion *in exchange for entry into Canada*.¹⁰¹

Justice L'Heureux-Dubé's concurring reasons in *Simmons* express a similar sentiment:

Individuals arriving at customs...in *electing* to travel outside the country or in seeking entry for the first time, have implicitly *chosen* to submit to the rules and procedures for leaving and entering the country. They expect, and are expected, to submit to a certain degree of inspection of their baggage, and in some cases, their person. Their situation is distinguishable from one where an individual is stopped or detained in the course of his or her normal activities within Canadian territory.¹⁰²

Underlying these courts' rationale for treating the border differently is the idea that, unlike situations where police arrest an individual or intrude upon his privacy at home, seeking entry to the country is an individual's *choice*. According to this theory, surrendering one's privacy to border agents is a price calculated to elicit a reward: permission to enter the country. The implication is that if people object to a random border search, then either they have something to hide or they do not seriously wish to enter. Neither is necessarily true. With all of the cultural, geopolitical, and socioeconomic imperatives that globalization brings, it is questionable to what extent presenting oneself for entry to the country can be described as a truly free or voluntary choice.¹⁰³ Furthermore, while travellers may "reasonably expect" that border agents will search their luggage, it is not clear that the same holds true of their digital devices. One need look no further than the media's bewilderment at Philippon's situation in order to appreciate the lack of consensus on this issue.

The tendency to treat border searches differently also appears to stem from their "random" and "routine" nature. For instance, Chief Justice Dickson held in *Simmons* that "[n]o 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."¹⁰⁴ Conducting groundless searches at the border is thus rendered reasonable in part by the fact that everyone is treated the same at the point of entry. However, the Ontario Court of Appeal conceded in *Jones* that, as a matter of fact, not all travellers *are* treated equally:

In a general sense, everyone who is questioned at the border and whose luggage is examined is the target of an investigation. Questions are asked and routine searches conducted to find individuals who are in breach of border-related laws. *It only makes good sense that those responsible for*

101 *Ibid* at para 30 [emphasis added].

102 *Simmons*, *supra* note 16 at para 85 [emphasis added].

103 See e.g. Ton van Naerssen & Martin van der Velde, "The Thresholds to Mobility Disentangled" in Martin van der Velde & Ton van Naerssen, eds, *Mobility and Migration Choices: Thresholds to Crossing Borders* (Dorchester, UK: Ashgate Publishing, 2015) 3 at 6. According to the authors, "the decision-making process that concerns mobility and migration movements needs to go beyond reductionist explanations that consider motivations to migrate as a matter of rational and measurable choice. That means, decision-making involves both cognitive and emotional processes...."

104 *Simmons*, *supra* note 16 at para 27.

*enforcing border regulations will focus their routine questions and searches on persons who have for some reason attracted their interest.*¹⁰⁵

If one accepts the Ontario Court of Appeal's statement as true, then border agents will not normally search an individual's cell phone or computer unless something triggers their suspicion. Therefore, the belief that *no* stigma attaches to the search of an individual's digital devices is debatable, especially when Chief Justice Dickson's comments did not specifically contemplate such devices in 1988.

Lastly, borders serve both literal and symbolic functions. They define a nation-state's territoriality, proclaim sovereignty, and determine a state's level of security against external threats depending on their "selective permeability."¹⁰⁶ Audrey Macklin, writing in the context of refugee policy, has argued that there is a disconnect between how Canadians imagine their borders and how they think of their communities.¹⁰⁷ On one hand, borders conjure up the image of an impenetrable fortress designed to keep foreign bodies out and to protect citizens from terrorism, narcotics, criminals, invasive species, and other things deemed undesirable. On the other hand, citizens like to think that Canada is an open and welcoming country in which differences and individual rights are respected. How the law treats computers at the border reflects the country's values. Respecting the privacy guarantee in section 8 is important in the customs context, not in spite of, but precisely because of the added pressure to search at the border. By treating the contents of digital devices with the same respect they warrant in other contexts, the law is shown in its best light.

D. A Better Constructive Interpretation

Law as integrity is anti-Archimedean in the sense that it does not contend that there is a single fixed point by which judges can find the correct interpretation of the law. Instead, judges explain the meaning of law by accounting for the legal system's underlying values.¹⁰⁸ I offer proportionality as the theme for a better constructive interpretation of a search's reasonableness under section 8, but not as a regulative principle taken from outside the law and foisted upon it. Rather, proportionality is posited as a theory that, taken as a principle of justice which runs throughout the jurisprudence and has the general explanatory power required by law as integrity, provides a more attractive way of telling the story behind section 8's treatment of digital devices in the best possible light.

To say that reasonableness "takes its colour from the context" is manifest.¹⁰⁹ This administrative law maxim is equally apparent in section 8. However, an examination of how courts currently assess the reasonableness of a search reveals that the *Collins* criteria for reasonableness (the search is authorized by law, the law itself is reasonable, and the search is conducted in a reasonable manner) lack the analytical rigour of reasonableness in other constitutional or administrative law contexts. For example, although section 8 is theoretically subject to the *Charter's* reasonable limits clause, the interest balancing that would normally occur at section 1 is practically contained within section 8. Indeed, it is unlikely that a court would hold that an *unreasonable* search could then be justified as a *reasonable* limit.¹¹⁰ The trouble is, beyond the relatively vague notion that a judge

¹⁰⁵ *Jones*, *supra* note 100 at para 40 [emphasis added].

¹⁰⁶ Audrey Macklin, "Borderline Security" in Ronald Daniels, Patrick Macklem & Kent Roach, eds, *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001) 383 at 383.

¹⁰⁷ *Ibid* at 384.

¹⁰⁸ Ripstein, *supra* note 60 at 9.

¹⁰⁹ *Canada (Citizenship and Immigration) v Khosa*, 2009 SCC 12 at para 59, [2009] 1 SCR 339.

¹¹⁰ Steven Penney, "Unreasonable Search and Seizure and Section 8 of the Charter: Cost-benefit Analysis in Constitutional Interpretation" (2013) 62 Sup Ct L Rev (2d) 101 at footnote 5.

must balance the interest of the individual against that of the state, the refined filter of proportionality provided by the *Oakes* test¹¹¹ is never applied in assessing a search's reasonableness. The result is a less robust reasonableness analysis without the quality control function that section 1 would ordinarily serve. Framing the issue in terms of finding the point at which the individual's interest in privacy must give way to that of the state, which finds its genesis in *Hunter*, misleadingly implies an inevitability: that there is always a point at which the individual's interest will give way. By contrast, asking whether an infringement of a right is *proportional* to the benefit to be obtained by the state is a more nuanced question, which seeks to accommodate both interests where feasible.

Precedent supports this approach. The proportionality project is an increasingly common constitutional narrative. In *R v NS*, the Supreme Court sought to strike a proportionate balance between a witness' freedom of religion and an accused's right to a fair trial, neither prohibiting a woman from wearing a niqab while testifying in court, nor universally condoning it.¹¹² More recently, in *Loyola High School v Quebec* ("*Loyola*") the Supreme Court considered whether a discretionary decision by the Minister of Education to deny Loyola High School an exemption from the provincially mandated Ethics and Religious Culture program was reasonable. The majority resolved the case by resort to the "robust" reasonableness standard in *R v Doré*,¹¹³ finding the denial infringed the school's freedom of religion more than necessary, while the dissenting justices would have allowed the appeal as an unreasonable limit under section 1 of the *Charter*.¹¹⁴ Although the Court split on the analytical approach to take, the reasonableness inquiry was the same: "did the Minister's decision limit Loyola's right to freedom of religion proportionately—that is, no more than was reasonably necessary?"¹¹⁵ The parallels between this question and the *Oakes* test are obvious. Asking the same question, which is analogous to the minimal impairment step in the *Oakes* test, in the context of section 8 is more likely to produce a just outcome because it brings coherence and thus integrity to the interpretation of reasonableness under the *Charter*. It would be incoherent if what qualifies as a reasonable limit implicit in section 8 were substantially dissimilar from what counts as a reasonable limit in section 1 simply because one provision focuses on proportionality, while the other does not. Hence, reasonableness-as-proportionality offers a better constructive interpretation of the law as a whole, making it easier to believe Dworkin's pretension that a single author wrote it and, most importantly, maximizing the odds that courts act justly when they apply it.

One might criticize this approach on the basis that it usurps the balancing function of section 1 and thereby creates an unworkable framework. For example, Graham Mayeda argues that section 8 should broadly protect privacy interests and that any assessment as to the reasonableness of a search should occur under the auspices of the *Oakes* test.¹¹⁶ He advocates a more flexible framework for evaluating breaches of privacy, criticizing the law's current approach to balancing an individual's privacy interests against countervailing state interests like security at section 8. Whether this balancing exercise should occur within section 8 or at section 1 deserves independent analysis; however,

111 See *R v Oakes*, [1986] 1 SCR 103 at 138–140, 53 OR (2d) 719.

112 *R v NS*, 2012 SCC 72, [2012] 3 SCR 726.

113 *Doré*, *supra* note 13.

114 *Loyola*, *supra* note 13.

115 *Ibid* at paras 31, 114. According to Aharon Barak, the former President of Israel's Supreme Court and a noted constitutional rights scholar, "Reasonableness in [a strong] sense strikes a proper balance among the relevant considerations and it does not differ substantially from proportionality" (quoted at para 38).

116 Graham Mayeda, "My Neighbour's Kid Just Bought a Drone...New Paradigms for Privacy Law in Canada" (2015) 35 NJCL 59 at 77–79.

the important point is that, as presently interpreted, section 8 leaves little to no room for section 1's proportionality analysis to work its magic, laying waste to the image of law as integrity and perpetuating significantly different—and potentially unjust—standards of reasonableness under the *Charter*. To the extent that law as integrity requires coherence with past judicial decisions, an approach that imports proportionality into section 8's internal assessment of a search's reasonableness better fits and justifies modern legal practice. A clear division of labour between sections 8 and 1 may be preferable from a practical perspective, but avoiding any overlap would require courts to revisit the seminal statements in *Hunter*, which launched the Court's emphasis on balancing individual and state interests under section 8.¹¹⁷

E. Proportionality as Integrity

On a conceptual level, proportionality theory and law as integrity share the same fundamental project. Dworkin's dimension of fit evokes an image of surgical precision in the law: of engineering an elegant solution to a legal problem that meets with the jagged, gap-toothed edge of the existing legal landscape, creating a perfect seal. Proportionality, by definition, seeks to achieve the same goal by finding the sweet spot at which the individual's interest in privacy and the state's interest in intruding upon that privacy are ideally balanced. Anything less than a proportional response is arbitrary to the extent that it is disproportional. Insofar as the arbitrary response impairs a right more than necessary, proportionality theory also holds that the limit is unreasonable.

Again, recall that an eligible constructive interpretation of the law does not have to fit every part of the historical text.¹¹⁸ In the same way, there may be more than one means to achieve a proportional balance. A proportional limit on a constitutional right must fall within a range of reasonable alternatives, what Aharon Barak terms the “zone of proportionality.”¹¹⁹ In the same way that the problem with the Minister's decision in *Loyola* was her assumption that teaching Catholicism from a Catholic perspective was “necessarily inimical”¹²⁰ to the state's core objective to foster openness and respect for diversity, the problem with the *Customs Act's* broad power to search goods is the assumption that any privacy protection for the contents of electronic devices is necessarily inimical to national security or the state's interest in self-protection. It is a simple matter of fact that even if the CBSA wanted to search every single electronic device that traverses its borders, the agency's limited resources prevent it from casting such a wide net. Therefore, as a matter of practical necessity, customs officials will typically (though not always) depend on the presence of reasonable grounds to suspect an individual has secreted something into the country before searching the digital contents of any electronics he might be carrying.¹²¹ Introducing the requirement that customs officials have reasonable suspicion before searching the contents of electronic devices is a modest protection that would more proportionally balance the individual's heightened privacy interest in his digital information and the state's interest in self-protection. This proposal formalizes what effectively happens on the ground already. The reasonable suspicion standard, which has historically applied to border searches of the person, requires objective, articulable facts that would lead a reasonable person to suspect a traveller may

117 See Lisa M Austin, “Information Sharing and the ‘Reasonable’ Ambiguities of Section 8 of the Charter” (2007) 57:2 UTLJ 499 at 510–512. Austin describes how courts sometimes conflate the reasonable expectation of privacy threshold question with the interest-balancing function of section 8 and discusses the risks that this creates.

118 Dworkin, *supra* note 10 at 230.

119 Aharon Barak, “Proportionality (2)” in Michel Rosenfeld & Andrés Sajó, eds, *The Oxford Handbook of Comparative Constitutional Law* (Oxford: Oxford UP, 2012) 738 at 748.

120 *Loyola*, *supra* note 13 at para 68.

121 Kugler, *supra* note 97 at 1178.

have contravened an Act of Parliament. It is not speculation, nor is it a hunch.¹²² Rather, it is a standard higher than mere suspicion and lower than reasonable and probable grounds.¹²³

One might argue that provisions like section 99(1)(a) of the *Customs Act* are necessary “when it is impossible to separate the narrower measures needed to realize the law’s purpose from those that are overinclusive.”¹²⁴ In other words, perhaps requiring individualized suspicion to search the contents of electronic devices at borders would not accomplish the legislative objective as effectively. Assuming for the sake of argument that this is true, the overinclusiveness of the customs search power vis-à-vis electronic devices may be dealt with in the final balancing act that proportionality requires. According to Barak, one must balance the social importance of the benefit to be gained from realizing the legislative objective (national security) against the social importance of avoiding the limitation on the right (privacy). Crucially, however, Barak emphasizes that this balancing—embodied in the last stage of the *Oakes* test—is not about comparing the overall importance of the objective to the overall importance of the right, but the *marginal social benefit* to be gained from *this particular law* with the *marginal harm* to the right.¹²⁵ This is an important insight because if privacy interests in the informational contents of electronic devices are compared to the objective of national security as a whole, as they have been in the section 8 jurisprudence until now, then privacy does not stand much chance at meaningful protection. However, the CBSA’s incapacity to actually search every electronic device that enters the country means that the marginal benefit to national security that may be gained from this power is no greater than it would be if the law restricted such searches to instances where officers had reasonable suspicion. Indeed, as Barak suggests, a less infringing alternative that does not accomplish the legislative objective equally as effectively may nonetheless represent a more proportional balance between the importance attached to the objective and to the right.¹²⁶

Barak also suggests that proportionality has a temporal aspect in the sense that its requirements are ongoing.¹²⁷ Similarly, law as integrity begins in the present. It requires a constructive interpretation according to which the past is relevant only to the extent that it fits with modern legal practice. In this sense, a constructive interpretation of section 8 based on proportionality need not abandon the legacy of *Simmons’* border exception altogether. This interpretation recognizes that the three categories crafted in 1988 may have been proportional and thus reasonable in light of technological and epistemological limits at that time. However, proportionality and integrity today both require an update to that old understanding in order to fit and justify modern legal practice. One might argue that transposing the kind of robust reasonableness analysis that the majority follows in *Loyola* or the rigours of the *Oakes* test to section 8 only makes explicit what was already implicit. However, Barak says proportionality must be orderly and transparent.¹²⁸ The current section 8 reasonableness analysis is both less orderly and less transparent than the interest balancing in *Loyola*. Like proportionality, integrity requires courts to engage with the law in a transparent manner. Therefore, a constructive interpretation of section 8’s reasonableness that mirrors the more robust understanding of proportionality in section 1 and in decisions like *Loyola*, and which

122 *R v Kang-Brown*, 2008 SCC 18 at paras 26, 76, [2008] SCR 456.

123 *Ibid* at para 75.

124 Barak, *supra* note 119 at 744.

125 *Ibid* at 745.

126 *Ibid*.

127 *Ibid* at 743.

128 *Ibid* at 749.

seeks to accommodate the privacy values underlying section 8 “as fully as possible,”¹²⁹ fits and justifies the law as a whole better than the anemic analysis that currently allows situational factors to dominate. This interpretation also holds that requiring reasonable suspicion before conducting a computer search at the border would more proportionally balance an individual’s privacy interests in the device’s contents with the interest of the state in intruding for purposes of national self-protection.

CONCLUSION

This paper began with a simple, yet powerful, proposition from Dworkin: that although acting with coherence does not guarantee justice, by doing so judges demonstrate their commitment *to* justice. Law as integrity does not free judges to decide cases on a whim; their interpretation is constrained to the extent that they must account for legal practice and what came before, if only to overrule or distinguish unhelpful precedent. While setting the threshold for fit is an inherently political exercise, it is not simply an abstract concept. It may be applied, as above, to illustrate the risk that incoherence will breed injustice. The informational contents of computers, such as laptops, tablets, smartphones, and other electronic devices, are recognized in law as engaging heightened privacy interests. That they attract a reasonable expectation of privacy sufficient to trigger the *Charter*’s protection under section 8 is clear. Interference with those contents by the state constitutes a search, which must be reasonable under the Constitution. The reasonableness of a content-related computer search is largely dictated by the situation in which it occurs. At home, police need a separate warrant. After arrest, police do not need a warrant but must have grounds for the arrest and the search must be related to the offence for which the individual was arrested. At the border, customs officers can turn on and search through a traveller’s electronics without any grounds whatsoever. This patchwork of reasonableness, where external circumstances are permitted to swoop in and trounce the individual’s privacy interest, does not strike a reasonable balance between state and individual interests to the extent that it is disproportional. Incoherence and its corresponding risk of injustice are exemplified by the law’s extension of the search incident to arrest doctrine to include electronic devices in *R v Fearon*. The majority opinion in that case offers a poor constructive interpretation of section 8’s reasonableness requirement, leaving major structural aspects of the written record unexplained.

A better constructive interpretation of the law on section 8 would provide a more reasonable balance in that context and at the border. Adopting proportionality theory as it has been developed under section 1 of the *Charter* and in *Loyola* is one such interpretation. Proportionality provides a compelling way to see the law in its best light because it runs through the jurisprudence and has general explanatory power. It also restores coherence to how reasonableness will be interpreted under the *Charter*, making it easier to conceive of the law as a coherent novel written by a single author. Powers under the *Customs Act* that empower border agents to search a computer’s contents without any grounds infringes an individual’s privacy more than reasonably necessary. A more proportional response that better balances the state and individual interests at stake would require reasonable suspicion before CBSA officials may search such devices. To be sure, customs officials have a difficult job. But the task of a judge faced with a case like Philippon’s is even harder: to make the law the best that it can be. When it comes to section 8, doing better is not only possible; it is proportional.

129 *Loyola*, *supra* note 13 at para 39.