COA-23-CR-0023
C70656

COURT OF APPEAL FOR ONTARIO

B E T W E E N :

S. David

Appellant

- and -

HIS MAJESTY THE KING

Respondent

- and -

CANADIAN CIVIL LIBERTIES ASSOCIATION, CRIMINAL LAWYERS ASSOCIATION (ONTARIO)

Interveners

A N D B E T W E E N :

HIS MAJESTY THE KING

Appellant

- and -

P. Jeremy

Respondent

- and -

CANADIAN CIVIL LIBERTIES ASSOCIATION, CRIMINAL LAWYERS ASSOCIATION (ONTARIO)

Interveners

INTERVENER'S FACTUM
CANADIAN CIVIL LIBERTIES ASSOCIATION

Samara Secter
Jocelyn Rempel
ADDARIO LAW GROUP LLP
101-171 John Street
Toronto, ON M5T 1X3
T: 416-649-5063
F: 1-866-714-1196
E. ssecter@addario.ca
jrempel@addario.ca

Lex Gill
TRUDEL JOHNSTON & LESPÉRANCE
750, Côte de la Place d'Armes, suite 90
Montréal, QC H2Y 2X8
T: 514-871-8385
F: 514 871-8800
E: lex@tjl.quebec

Counsel for the Intervener, Canadian Civil Liberties Association

TO: Michael Fawcett
Rebecca De Filippis
Crown Law Office - Criminal
720 Bay Street, 10th floor
Toronto, Ontario
M7A 2S9
Tel: 416-326-2307
Fax: 416-326-4656
E: michael.fawcett@ontario.ca
rebecca.defilippis@ontario.ca

Counsel for the Attorney General of Ontario

AND TO: Naomi Lutes
Greenspan Humphrey Weinstein
15 Bedford Road
Toronto, Ontario
M5R 2J7
Tel. 416-868-1755
Fax 416-868-1990
E: nml@15bedford.com

Counsel for the Appellant, S. David

AND TO: Daisy McCabe-Lokos

McCabe-Lokos Law
405-700 Bay St.
Toronto, Ontario
M5G 1Z6
Tel. 647-531-9223
Fax 647-494-7712
E: daisy@mccabelokoslaw.com

Counsel for the Appellant, P. Jeremy

AND TO:

Ian Bell
Jennifer Conroy
Public Prosecution Service of Canada
201 County Court Blvd.
Suite 600
Brampton, ON L6W 4L2
Tel: 905-454-2424
Fax: 905-454-2168
E: ian.bell@ppsc-sppc.gc.ca ;
jennifer.conroy@ppsc.sppc.gc.ca

Counsel for the Attorney General of Canada

AND TO:

Nader Hassan
Spencer Bass
Stockwoods LLP
TD North Tower
77 King Street West, Suite 4130
Toronto, ON M5K 1H1
Tel: 416-593-1668
Fax: 416-593-9345
E: naderh@stockwoods.ca
spencerb@stockwoods.ca

Counsel for the Intervener, Criminal Lawyers' Association

AND TO:

The Registrar
Court of Appeal for Ontario

PART I – OVERVIEW

1. Any proposed interpretation of the search power in s. 99(1)(a) of the *Customs Act* that allows for standardless, limitless searches of electronic devices is out of touch with the reasonable expectations of Canadians and contravenes the *Charter*. If interpreted in this manner, the provision treats personal electronic devices at the border as though they are physical recepticals like suitcases or purses, even though our Supreme Court has explicitly rejected that approach.[1] In reality, our electronic devices are a limitless trove of our most personal, intimate, and sensitive information. Any search of these devices should be circumscribed by a stringent standard and clear legislative safeguards.

2. The CCLA submits that travelers' reasonable expectation of privacy in their electronic devices requires robust constitutional protection. If standardless, limitless searches are authorized by s. 99(1)(a) of the *Customs Act*, they unreasonably interfere with our reasonable expectations of privacy. The sweeping powers given to Border Services Officers (BSOs) under the *Customs Act* transform the border into a *Charter* free zone. In order for border searches of personal electronic devices to be constitutional, the CCLA submits there must be both: (a) a legislated, constitutional standard BSOs must meet before searching a traveler's electronic device; and (b) clear guidelines for the manner in which those searches are conducted. The CCLA also proposes guidelines necessary for a BSO to search a personal device, should Parliament implement a constitutional standard.

PART II – STATEMENT OF FACTS

3. The Canadian Civil Liberties Association (the "CCLA") takes no position on the facts.

---

[1] *R. v. Fearon*, 2014 SCC 77, at para. 51.

PART III – POSITION ON QUESTIONS IN ISSUE

4. The CCLA argues that the standardless, limitless searches of travelers' electronic devices at the border breaches s. 8 of the *Charter* and, to the extent that s. 99(1)(a) of the *Customs Act* purports to authorize such searches, the provision is unconstitutional.

5. The CCLA takes no position on any other grounds of appeal.

PART IV – STATEMENT OF ARGUMENT

A. Canadian Law Requires Heightened Standards for Searching Electronic Devices

6. Standardless, limitless searches of electronic devices are unconstitutional in Canadian law because of the heightened privacy interest in individuals' personal electronic devices. The Supreme Court has long recognized the unique type of privacy that people have in their digital devices and digital footprints:

- *R. v. Morelli*, 2010 SCC 8: "It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer."[2]
- *R. v. Vu*, 2013 SCC 60: "The privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets. Computers potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search."[3]
- *R. v. Fearon*, 2014 SCC 77: "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"…[i]t is unrealistic to equate a cell phone with a briefcase or document found in someone's possession at the time of arrest."[4]

---

[2] *R. v. Morelli*, 2010 SCC 8, at para. 2.
[3] *R. v. Vu*, 2013 SCC 60, at para. 24.
[4] *R. v. Fearon*, 2014 SCC 77, at para. 51.

- *R. v. Bykovets*, 2024 SCC 6: "[IP addresses] are the key to unlocking an Internet user's online activity — the first "digital breadcrumbs" on the user's cybernetic trail…[t]hose breadcrumbs may establish an Internet user's entire daily, weekly, or even monthly online activity, leading to an electronic roadmap… [l]ike the computer in *Reeves*, an IP address provides the state with the means that can lead them to a trove of personal information."[5]

7. These comments also echo Harris J.'s observation in *Pike*: "A search of the data in a personal digital device…digs deep into the heart of who we are."[6]

8. Canada recognizes only two circumstances where police can search an individual's personal electronic device: (a) with a warrant, requiring reasonable and probable grounds; or (b) for highly circumscribed purposes upon lawful arrest, which itself requires reasonable and probable grounds. Police executing a warrant on a residence can search inside cupboards and closets, but require specific prior authorization to search a computer or cell phone.[7] Similarly, while police can search a purse incident to arrest, there are strict guidelines for when and how to search a cellphone in the same circumstances.[8] Allowing for standardless searches at the border is inconsistent with the rest of our jurisprudence.[9]

9. Any American case law that embraces standardless, limitless searches at the border as constitutional should not be followed for at least three reasons. First, s. 8 of the *Charter* does not follow the same logic as the U.S. Fourth Amendment. As far back as 1995, our Supreme Court noted that Canada takes a "more protective attitude towards individual privacy" than the United States.[10] The Supreme Court has also cautioned against transplanting Fourth Amendment

---

[5] *R. v. Bykovets*, 2024 SCC 6, at para. 69.
[6] *R. v. Pike*, 2022 ONSC 2297, at para. 53.
[7] *R. v. Vu*, 2013 SCC 60, at paras. 38, 64.
[8] *R. v. Fearon*, 2014 SCC 77, at para. 83.
[9] This factum does not opine on the wisdom of standardless luggage searches. The CCLA only notes the important distinctions between luggage and personal electronic devices.
[10] *R. v. Silviera*, [1995] 2 S.C.R. 297, at 325.

principles into Canadian law.[11] Second, all U.S. constitutional rights are interpreted with the automatic exclusionary rule in mind. Unlike in Canada where the exclusion of evidence following a breach involves a balancing exercise under s. 24(2),[12] evidence in the U.S. is automatically excluded following a breach. As a result, the U.S. takes a narrower approach to avoid excluding evidence arising from minor breaches. Third, the U.S. jurisprudence is not settled regarding the standard required for device searches at the border.[13] As it is still evolving, American law has not been tested such that it is a stable and informative comparator to draw upon.[14]

B. People Are Not Required Become "Digital Recluses" or to Stay Home to Maintain Privacy

10. This Court should reject the argument that the "choice" to cross the border with an electronic device means travelers must subject themselves to the risk of a standardless, limitless search of any device they carry with them. This framing of travelling with a device as a "choice"[15] revives the "risk analysis" rejected by the Supreme Court in *Duarte*, *Wong*, *Jones*, and *Marakah*.[16] The risk analysis runs contrary to the Supreme Court's normative approach. Section 8 protects privacy, not isolation.[17] It is the state's burden to establish constitutional search powers, not the individual's burden to avoid scenarios where they may be unconstitutionally searched.

---

[11] *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145, at 161.
[12] Ie. the 3-step *Grant* test.
[13] Appellate courts are split on whether customs officials need reasonable suspicion to do a forensic search of a device. 4th circuit (Virginia, Maryland, North Carolina) and 9th circuit (California, Alaska, Arizona, Hawaii, Idaho, Montana, Nevada, Oregon, Washington) courts require reasonable suspicion for forensic searches of devices: *United States v. Kolsuz*, 890 F.3d 133, 136 (4th Cir. 2018); *United States v. Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019). The 11th circuit (Alabama/Florida/Georgia) does not require reasonable suspicion for forensic searches of devices: *United States v. Touset*, 890 F.3d 1227, 1229 (11th Cir. 2018).
[14] See eg. in May 2023 in the Southern District of New York, Justice Rakoff found that customs officials need a warrant, supported by reasonable cause, to do a forensic search of a device at the border: *United States v. Smith*, 2023 WL 3358357 (S.D.N.Y. 2023).
[15] Factum of the Appellant (the Attorney General of Ontario), Pike Appeal, at para. 41.
[16] *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Wong*, [1990] 3 S.C.R. 36; *R. v. Jones*, 2017 SCC 60; *R. v. Marakah*, 2017 SCC 59.
[17] *R v. Spencer*, 2014 SCC 43, at para. 15.

i. Digital Privacy is Necessary for Meaningful Participation in Society

11. The ability to move across the border without being subjected to unjustified state intrusion into our personal devices is vital to a free and healthy society. Our s. 8 standards must reflect our our law with respect to digital privacy.[18] Although referring to the internet, the following comments from Karakatsanis J. in *Bykovets* are equally applicable to our electronic devices, which have:[19]

> "[B]ecome a constant companion, through which we confide our hopes, aspirations, and fears. Individuals use [their phones] not only to find recipes, pay bills, or get directions, but also to explore their sexualities, to map out their futures, and to find love."

When phones became our "constant companions", our *Charter* evolved to reflect that reality.

12. Electronic devices provide a myriad of ways for self-fulfillment and expression. They allow people to reach beyond their immediate surroundings and form relationships and communities with others around the world. They enable debate. Protecting a zone of privacy for electronic devices allow individuals to make meaningful choices about their participation in society: "A private inner life is essential to the autonomous individual that forms the basis of a free and democratic society as envisioned by the *Charter*."[20] Fear of constant state intrusion or supervision diminishes individuals' freedom.[21]

13. In order to justify interferences with the right to privacy, the Court must ask whether the intrusion would see individuals' freedoms "diminished to a compass inconsistent with the aims of free and open society."[22] In this case, a judgment permitting BSOs to conduct standardless, limitless searches of our "constant companions" would. As the Supreme Court confirmed in *Jones*,

---

[18] *R v. Tessling*, 2004 SCC 67, para. 42; Stewart, H. "Normative Foundations for Expectations of Privacy", (2011) 54 SCLR (2d) 335 at 342-343; *R v.Orlandis-Hagsburo*, 2017 ONCA 649, at para. 41.
[19] *R. v. Bykovets*, 2024 SCC 6, at para. 1.
[20] *R. v. Fearon*, 2014 SCC 77, *per* Karakatsanis J. (in dissent but not on this point), at para. 115.
[21] *R v. Patrick*, 2009 SCC 17, at para. 14.
[22] *R v. Wong*, [1990] 3 SCR 36, at para. 12.

"Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives."[23] Nor are they required stay home, never exploring the world beyond their borders.[24]

ii. Unconstitutional Border Searches Force Canadian Travelers to Choose Between Privacy and Mobility

14. The searches authorized by s. 99(1)(a) are unconstitutional in relation to all travelers, regardless of citizenship. However, for Canadian travellers, they also represent an interference with the s. 6 right to freely cross Canada's borders. The result of the Crown's suggested approach is that individuals who cannot leave their devices at home, but want to avoid state intrusion, must give up their right to travel.

15. In this manner, the Crown's position forces Canadians to choose between at least two constitutional rights — the right to be free from unreasonable search and seizure (s. 8) and the right to enter and leave Canada (s. 6(1)). Mobility rights under s. 6(1) are a fundamental right associated with citizenship which ensure that Canadians can freely leave any country and will not be arbitrarily deprived of the right to enter Canada.[25] When international travel is rendered conditional on the assertion that one's private life can be subject to unlimited, arbitrary and unjustified scrutiny, that freedom is diminished. Canadian travellers face an impossible choice.

16. The choice is impossible because access to a computer and cell phone is essentially required — both at home and abroad — to access basic services, to carry out financial transactions, to navigate, to work, and to communicate. People traveling for work now routinely carry laptops or tablets carrying sensitive personal and client information, including lawyers travelling with

[23] *R v. Jones*, 2017 SCC 60, at para. 45.
[24] *R. v. Duarte*, [1990] 1 S.C.R. 30, at pp. 48-49.
[25] *Divito v. Canada (Minister of Public Safety and Emergency Preparedness)*, 2013 SCC 47, at paras. 21, 25.

client's evidence, judges with draft judgments, doctors with patient health records, and journalists with source material. Children also carry laptops or tablets for schoolwork and entertainment. It is unfeasible and unprincipled to suggest that, in order to maintain privacy, travelers must have the technical know-how to wipe their devices or transfer the contents before travelling lest they risk unrestricted searches at the border.[26] Travelers should not have to choose between their right to cross the border and their right to be free from invasions of digital privacy at the border.

C. The Reduced Expectation of Privacy at the Border makes Limited Sense in the Context of Electronic Devices

17. Section 99(1)(a) was enacted in 1985, long before personal electronic devices became prevalent.[27] Parliament could have never intended, or even predicted, that the provision could authorize the kind of privacy intrusion the Crown now claims to be lawful. Parliament indicated its intention to protect private communications by requiring reasonable suspicion for BSOs to open a letter[28] — a search that is far less intrusive, both qualitatively and quantitatively, than a search of an electronic device. Parliament could not have foreseen the need to protect the digital devices of today. [29]

18. Section 99(1)(a) aims to protect Canada from physical threats being brought over the border, as contemplated in *Simmons*, *Monney*, and *Jones*.[30] In all three decisions, the searches related to the secreting of drugs on one's person or luggage when crossing the border. These cases recognized that there was a lower expectation of privacy at the border in physical items hidden on

---

[26] Indeed, encouraging wiping is a work-around of the very goal the Crown suggests Parliament has.
[27] "Crossing the line? The CBSA's Examination of Digital Devices at the Border", Office of the Privacy Commissioner of Canada (October 21, 2019), at para. 106.
[28] *Customs Act*, 99(1)(b), (c.1).
[29] The CCLA does not concede that the definition of "goods" in the *Customs Act* includes electronic devices. The CCLA relies on the factum of the Criminal Lawyers' Association and agrees that electronic devices are not captured as "goods". However, if they are, a standard and limits are required to search electronic devices.
[30] *R. v. Simmons*, [1988] 2 S.C.R. 495; *R. v. Monney*, [1999] 1 S.C.R. 652; *R. v. Jones*, [2006] O.J. No. 3315 (C.A.).

your person or in your luggage because of the interest in keeping physical contraband outside of Canada. The underlying principle is that the border is a uniquely important place to intercept physical contraband.

19. By contrast, the idea that border searches are necessary to stop the flow of illegal electronic content is undermined by the basic functioning of the Internet. Data is not a physical good that can be stopped at the border. [31] Electronic data is not secreted upon one's person or in their luggage. There is no electronic data stored on a device crossing the border that cannot make its way into the country by other means; information can be transferred through the internet from one jurisdiction to another instantaneously, at any time, without ever going near a border or encountering a customs official.[32] As a result, searches of electronic devices at the border has only a marginal connection to the legislative objective of preventing the flow of contraband. This reality is recognized by specialized police units dedicated to ferreting out crime on the internet across borders, such as internet child exploitation units. Unlike physical goods that can be intercepted at an airport or land crossing, the internet knows no borders.

20. The fundamental differences between electronic data and physical goods requires a difference in the expectation of privacy each is afforded. Individuals have a much higher expectation of privacy in their electronic devices because they contain immense amounts of highly private information.[33] As the Supreme Court recognized in *Fearon*, the data storage capacity of electronic devices can "vastly exceed what an individual could carry on their person or in a

---

[31] See *R. v. Canfield*, 2020 ABCA 383, at para. 48: note that CBSA's practice is to put devices in airplane mode — i.e., to disable internet connection entirely — prior to conducting the search, presumably both to prevent "remote wiping" and because even CBSA's interpretation of "goods" cannot extend to data that is not stored on the device.
[32] *R. v. Cole*, 2012 SCC 53, at para. 109. See eg. *R. v. Cusick*, 2019 ONCA 524, at paras. 5, 22-23: child pornography is transmitted via the cloud.
[33] *R. v. Fearon*, 2014 SCC 77, at paras. 126-27.

briefcase."[34] Neither a briefcase or a suitcase has the storage or potential to reveal as much intimate information as our cell phones and laptops.

21. The practical effect of the provision is that in order to avoid state scrutiny, travellers must wipe the sensitive data on their electronic devices before crossing the border and then re-download the same information after clearing customs. This kind of requirement imposes a significant inconvenience on ordinary travellers and makes access to basic privacy rights directly contingent on one's degree of technical sophistication. Such a functional requirement is arbitrary, burdensome, and achieves no security benefit for Canada.

22. While Canada has a compelling interest in controlling the flow of physical goods across its borders, this must be distinguished from any interest it has in controlling the flow of *information* across its borders or in accessing the private information of people who cross its borders. Information often does not exist in a single physical location and can often be accessed from many different locations, sometimes simultaneously. An email viewable on a smartphone might exist on multiple servers and might be accessible from various different smartphones and computers at any given time. It might be accessible from any computer in the world that is connected to the Internet provided the right login information is provided. The data is not imported into Canada just because one of the devices that can access the data crosses the Canadian border, just as a Canadian sitting at their desk in Toronto who receives an email sent from outside Canada has not imported the content of the email into Canada. The broad goods-importation paradigm in s. 99(1)(a) does not reflect the realities of electronic data storage, transmission, and use — all of which transcend the physical border.[35]

---

[34] *R. v. Fearon*, 2014 SCC 77, at para. 128.
[35] "Crossing the line? The CBSA's Examination of Digital Devices at the Border", Office of the Privacy Commissioner of Canada (October 21, 2019), at para. 106.

23. Indeed, the Supreme Court of Canada has repeatedly recognized this modern reality: that electronic information accessible through a smartphone or computer is not located at the location of the device itself. In *Vu*, the Court stated that

> …when connected to the Internet, computers serve as portals to an almost infinite amount of information that is shared between different users and is stored almost anywhere in the world… [A] search of a computer connected to the Internet or a network gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized [Emphasis added].[36]

The Court reiterated this distinction and confirmed its application to cellphones in *Fearon*.[37]

24. When a traveler carries a smartphone across the border, information in or accessible through the smartphone is not itself only at the border. The state should not be granted *carte blanche* to search citizens' pre-existing electronic information whenever they arrive at the border with a mobile device simply because the device can *access* this pre-existing information. Such a rule far overshoots the mischief and legitimate security concerns at which the border protection scheme is aimed.

D. Calling s. 99(1)(a) a Regulatory Power Does not Make Warrantless, Limitless Searches of Electronic Devices Reasonable

25. This Court should give no weight to the argument that BSOs exercise regulatory power under s. 99(1)(a) of the *Customs Act* as opposed to a criminal law power. First, the regulatory vs. criminal law power distinction is unhelpful in this case because it is not clear that the power exercised by BSOs is solely regulatory. Second, even if the *Customs Act* is regulatory, that categorization cannot constitutionalize a standardless, limitless search of electronic devices.

---

[36] *R. v. Vu*, 2013 SCC 60, at para. 44.
[37] *R. v. Fearon*, 2014 SCC 77, at para. 51.

26. BSOs searching electronic devices for criminal contraband under s. 99(1)(a) are not only exercising a regulatory power. In the present two appeals, the searches were conducted by BSOs looking for child pornography on electronic devices. As a result, the purpose of the search power exercised in these circumstances was criminal in nature.

27. However, even if the search power under s. 99(1)(a) is regulatory like the Crown suggests, the high expectation of privacy in the contents of an electronic device makes any standardless, limitless search of a device unreasonable — regardless of the statutory classification of regulatory or criminal. In *Jarvis*, the Supreme Court was asked to make a determination about whether the *Income Tax Act* exercised regulatory or criminal law power. The Court declined to make a final determination, instructing, "[w]hat is ultimately important are not labels [regulatory vs criminal] (though these are undoubtedly useful), but the values at stake in the particular context."[38] The same is true here. Assuming the *Customs Act* is regulatory does not end the analysis — the values at stake in this context cut to the core of privacy in a digital age. *Hunter v. Southam* is another example.[39] Although the statute in question in *Hunter*, the *Combines Act*, was largely regulatory, this was not determinative. The regulatory nature of the scheme did not mean that all state actions were justified or that constitutional standards were necessarily lower. The Court found that warrantless searches for documents in residences or businesses were nonetheless contrary to s. 8 The intrusive nature of searching through one's home or business required the state to have prior authorization to justify the privacy invasion.

28. What is at stake here is the right to maintain privacy over highly personal information — free from invasive, unjustified searches. Electronic devices hold a wealth of personal information for which individuals have a high degree of privacy. The fundamental privacy interest individuals

---

[38] *R. v. Jarvis*, 2002 SCC 73, at para. 61.
[39] *Hunter et al. v. Southam*, [1984] 2 S.C.R. 145.

have in the content of their devices has been upheld by the Supreme Court repeatedly.[40] Even a flexible approach to s. 8 leads to the conclusion that standardless, limitless searches of electronic devices are unreasonable based on the values at stake.

29. The caselaw the Crown cites to support the constitutionality of regulatory schemes is not applicable here.[41] Searching a personal electronic device is significantly more intrusive than the searches at issue in those cases. A number of the cases cited are those where the state sought to seize items for which the Court found those individuals had a low expectation of privacy, such as business records and documents created specifically for the financial regulatory scheme used to authorize the seizure[42] or documents supporting income tax filings.[43] Furthermore, those regimes require the production of business documents, not a physical invasion of one's personal property. The Court in *McKinlay* noted this difference when differentiating between tax officials demanding documents vs entering a taxpayer's house to search:"[t]he greater the intrusion into the privacy interests of an individual, the more likely it will be that safeguards akin to those in *Hunter* will be required."[44] Individuals have a much greater expectation of privacy when their personal property is invaded,[45] requiring more safeguards for their search. The search of an electronic device is incomparable to the above examples based on the level of invasion and the level of personal privacy violated through the search.

---

[40] *R. v. Morelli*, 2010 SCC 8, at para. 2; *R. v. Vu*, 2013 SCC 60, at para. 24; *R. v. Fearon*, 2014 SCC 77, at para. 51; *R. v. Bykovets*, 2024 SCC 6, at para. 69.
[41] Factum of the Intervenor (Public Prosecution Service of Canada), Pike Appeal, paras. 33-35.
[42] *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Practices Commission)*, [1990] 1 S.C.R. 425; *British Columbia Securities Commission v. Branch*, [1995] 2 S.C.R. 3.
[43] *R. v. McKinlay Transport Ltd.*, [1990] 1 S.C.R. 627, at 649-50.
[44] *R. v. McKinlay Transport Ltd.*, [1990] 1 S.C.R. 627, at 649.
[45] *R. v. McKinlay Transport Ltd.*, [1990] 1 S.C.R. 627, at 649. See also eg. *Hunter et al. v. Southam*, [1984] 2 S.C.R. 145.

E. The Section 8 Breach Cannot be Saved Under Section 1

30. The CCLA makes two points regarding the s. 1 analysis: (1) the internal CBSA policy manual that interprets s. 99(1)(a) by directing BSOs to undertake standardless, limitless searches of electronic devices is not a limit prescribed by law; and (2) at the final balancing stage, the low-visibility nature of the searches at issue and disproportionate impact on marginalized individuals is a significant deleterious effect.

31. Section 99(1)(a) contains no legislative limit on the search of goods — including electronic devices — at the border.[46] This Court should reject any suggestion that the CBSA's internal policy manual which interprets s. 99(1)(a) can stand in as a limit prescribed by law. The CBSA policy manual is simply an administrative document intended to guide BSOs in searching electronic devices without warrants or standards. Administrative policies are not limits prescribed by law.[47] No statute authorizes the CBSA manual.[48] The rules and investigative suggestions it contains are not binding.[49] The manual is informal, for internal use, is not readily accessible to the public, and does not come from or require public input.[50] The Standing Committee on Access to Information, Privacy, and Ethics even found that the CBSA's policies cannot be enforced because they do not have the force of law.[51] There is no support for the suggestion that the CBSA manual is a legislative policy such that it dictates a limit prescribed by law. The state cannot justify the s. 8 breach under s. 1 because it cannot point to a limit prescribed by law.

---

[46] *R. v. Canfield*, 2020 ABCA 383, at paras. 96-97; *R. v. Pike and Scott*, 2022 ONSC 2297, at paras. 111-14.
[47] *Canadian Federation of Students v. Greater Vancouver Transportation Authority*, 2009 SCC 31, at paras. 63-64; *Little Sisters Book and Art Emporium v. Canada (Minister of Justice)*, 2000 SCC 69, at para. 85.
[48] *Canadian Federation of Students v. Greater Vancouver Transportation Authority*, 2009 SCC 31, at para. 65.
[49] *Canadian Federation of Students v. Greater Vancouver Transportation Authority*, 2009 SCC 31, at para. 64.
[50] *Canadian Federation of Students v. Greater Vancouver Transportation Authority*, 2009 SCC 31, at para. 63.
[51] "Crossing the line? The CBSA's Examination of Digital Devices at the Border", Office of the Privacy Commissioner of Canada (October 21, 2019), at paras. 144-45.

32. At the final balancing stage, this Court should consider the deleterious effect of the "low visibility" searches the Crown suggests are allowed under s. 99(1)(a). There is insufficient independent oversight of the BSOs involved. This means that the provision as proposed by the Crown will have a particular impact on law-abiding individuals and be evasive of meaningful review. On the Crown's version, the statute enables police to interfere with the privacy and liberty of someone who they accept is acting lawfully and they do not even suspect or believe is about to or has committed an offence. As the Supreme Court stated: "it is especially important for the courts to guard against intrusions on the liberty of persons who are neither accused nor suspected of committing any crime."[52]

33. Another factor that should be considered in the overall balancing stage is that limitless, standardless searches disproportionately affect the most vulnerable in our society. This kind of highly discretionary, low visibility search power often targets the most marginalized.[53] For example, BSOs may stop people coming from certain countries to search their devices simply because of myths and stereotypes about that country — reinforcing stereotypes and targeting minority individuals. BSOs may also initiate searches of people's devices because they display characteristics that they think are suspicious, such as being nervous. Marginalized individuals may appear nervous around authority figures for precisely the same the reason why they are being searched — unchecked officer discretion. The targeting of the vulnerable is a significant deleterious effect of s. 99(1)(a).

[52] See, eg. *Fleming v. Ontario*, 2019 SCC 45 at paras. 76-78
[53] See eg. Report of the Independent Street Checks Review, the Honourable Michael H. Tulloch, 2018; *R. v. Le*, 2019 SCC 34, at para. 87.

F. Proposed Guidelines for Executing Searches on Electronic Devices at the Border

34. Parliament needs to ensure that the any regime for searching electronic devices at the border creates: (a) a sufficiently high legislative standard for a search that recognizes the necessity of travel and electronic device usage as well as the privacy interests our personal devices hold; and (b) clear guidelines for how a BSO executes the search. With respect to the standard, our normative expectations — confirmed by recent appellate jurisprudence — trends toward recognizing the importance of privacy in our digital age. As a result, it is hard to imagine a scenario where anything less than reasonable grounds to believe is the appropriate standard for searching electronic devices.

35. Investigative searches of electronic devices at the border require clear limits to respect the ss. 8, 9, 10(a), and 10(b) *Charter* rights of travelers because they are detained to have their device searched. Once a BSO determines that they have the requisite grounds to search at large through a traveler's electronic device, the traveler is detained. The traveler is detained because the BSO is no longer conducting "routine" searching, such as administering an x-ray, asking questions about marital status, or glancing at a receipt displayed on a phone screen.[54] The BSO's actions setting the search in motion objectively indicate that the traveler is not free to refuse and go on their way[55] — the BSO informs the traveler that their device will be searched, they take the traveler into a separate room, they seize the device, and then they start sifting through the traveler's highly private information stored on their electronic device. A traveler in that situation does not feel free to go.

---

[54] *R. v. Ceballo*, 2021 ONCA 791, at para. 21. See also *R. v. Canfield*, 2020 ABCA 383, at para. 128-29.
[55] *R. v. Ceballo*, 2021 ONCA 791, at para. 29.

36. Where a BSO can: (a) meet the standard to search set by Parliament; and (b) assuming that standard is constitutional, the CCLA proposes these additional guidelines to limit a BSO's search of an electronic device including:

1. The BSO must advise the traveler that they are detained and give the traveler their rights to counsel prior to the search under s. 10(b) of the *Charter*;

2. The BSO must allow a reasonable opportunity for the traveler to contact counsel;[56]

3. The BSO must allow the traveller to turn off the cellular and wifi capability of the device before searching, so as not to intercept communications as they are received or access any information that is not locally stored on the device itself (which would exceed the concept of a "good" under the *Act*);[57]

4. The BSO must articulate the specific purpose of the search prior and then tailor the nature and extent of their search to the purpose (ie. if the BSO is looking for evidence that the traveller has a particular license or receipt, they should not search a folder on a laptop containing family photographs);[58]

5. The BSO must keep detailed notes of their search pathways on the device and their findings — these notes should be made available to the individual to facilitate public accountability and any s. 24(1) remedy sought, whether a charge follows the search or not;[59] and,

6. The BSO must cease the search if they locate an illegal item and seek a warrant, or turn the matter over to police to seek a warrant, because any further searching for the purpose of collecting evidence for a prosecution is outside the customs mandate.[60]

37. Rights are not — and cannot be — suspended at the border. Standards and limits need to be put in place to ensure BSOs do not trample travelers' fundamental constitutional freedoms.

---

[56] Regardless of the legal test, if the device is password protected or encrypted, BSOs cannot force individuals to provide a password or otherwise compel them to facilitate the search on their own device. This would violate their right against self-incrimination under s. 7: see eg. *R. c. Boudreau-Fontaine*, 2010 QCCA 1108.
[57] While the CCLA does not accept that digital data stored on electronic devices is a "good", information stored remotely is even further removed from the definition of a "good" and certainly should not be considered as such.
[58] *R. v. Fearon*, 2014 SCC 77, at para. 83.
[59] *R. v. Fearon*, 2014 SCC 77, at para. 83.
[60] *R. v. Singh*, 2019 ONCJ 453, at paras. 85-86. This is not a complete list of necessary steps to protect privacy. It is only the beginning of an articulation of requirements to ensure that travellers' privacy is fairly protected even at the border.

PART V – ORDER REQUESTED

38. The CCLA takes no position on the disposition of these appeals.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 11th day of March, 2024.

Samara Secter
Jocelyn Rempel
ADDARIO LAW GROUP LLP
101-171 John Street
Toronto, ON M5T 1X3
T: 416-649-5063
F: 1-866-714-1196
E. ssecter@addario.ca
jrempel@addario.ca

Lex Gill
TRUDEL JOHNSTON & LESPÉRANCE
750, Côte de la Place d'Armes, suite 90
Montréal, QC H2Y 2X8
T: 514-871-8385
F: 514 871-8800
E: lex@tjl.quebec

Counsel for the Intervener, Canadian Civil Liberties Association

SCHEDULE A – AUTHORITIES CITED

R. v. Fearon, 2014 SCC 77

R. v. Morelli, 2010 SCC 8

R. v. Vu, 2013 SCC 60

R. v. Bykovets, 2024 SCC 6

R. v. Pike, 2022 ONSC 2297

R. v. Silviera, [1995] 2 S.C.R. 297

Hunter et al. v. Southam Inc., [1984] 2 S.C.R. 145

United States v. Kolsuz, 890 F.3d 133, 136 (4th Cir. 2018)

United States v. Cano, 934 F.3d 1002, 1007 (9th Cir. 2019)

United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018)

United States v. Smith, 2023 WL 3358357 (S.D.N.Y. 2023)

R. v. Duarte, [1990] 1 S.C.R. 30

R. v. Wong, [1990] 3 S.C.R. 36

R. v. Jones, 2017 SCC 60

R. v. Marakah, 2017 SCC 59

R v. Spencer, 2014 SCC 43

R v. Tessling, 2004 SCC 67

R v.Orlandis-Hagsburo, 2017 ONCA 649

R v. Patrick, 2009 SCC 17

Divito v. Canada (Minister of Public Safety and Emergency Preparedness), 2013 SCC 47

R. v. Simmons, [1988] 2 S.C.R. 495

R. v. Monney, [1999] 1 S.C.R. 652

R. v. Jones, [2006] O.J. No. 3315 (C.A.)

R. v. Canfield, 2020 ABCA 383

R. v. Cole, 2012 SCC 53

R. v. Cusick, 2019 ONCA 524

R. v. Jarvis, 2002 SCC 73

Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Practices Commission), [1990] 1 S.C.R. 425

British Columbia Securities Commission v. Branch, [1995] 2 S.C.R. 3

R. v. McKinlay Transport Ltd., [1990] 1 S.C.R. 627

Canadian Federation of Students v. Greater Vancouver Transportation Authority, 2009 SCC 31

Fleming v. Ontario, 2019 SCC 45

Little Sisters Book and Art Emporium v. Canada (Minister of Justice), 2000 SCC 69

R. v. Le, 2019 SCC 34

R. v. Ceballo, 2021 ONCA 791

R. c. Boudreau-Fontaine, 2010 QCCA 1108

R. v. Singh, 2019 ONCJ 453

SCHEDULE B – LIST OF STATUTES

Customs Act, R.S.C. 1985, c.1, s. 99(1)(a), (b)

Examination of goods

99 (1) An officer may

(a) at any time up to the time of release, examine any goods that have been imported and open or cause to be opened any package or container of imported goods and take samples of imported goods in reasonable amounts;

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

B E T W E E N :

HER MAJESTY THE QUEEN Appellant/Respondent	and	S. DAVID (Appellant) P. JEREMY (Respondent)	and	CANADIAN CIVIL LIBERTIES ASSOCIATION, CRIMINAL LAWYERS ASSOCIATION Interveners	Court File Nos: COA-23-CR-0023; C70656

IN THE ONTARIO COURT OF APPEAL
(ON APPEAL FROM THE ONTARIO SUPERIOR COURT OF JUSTICE)

INTERVENER'S FACTUM, CANADIAN CIVIL LIBERTIES ASSOCIATION

Samara Secter
Jocelyn Rempel
ADDARIO LAW GROUP LLP
101-171 John Street
Toronto, ON M5T 1X3
T: 416-649-5063
F: 1-866-714-1196
E. ssecter@addario.ca
jrempel@addario.ca

Lex Gill
TRUDEL JOHNSTON & LESPÉRANCE
750, Côte de la Place d'Armes, suite 90
Montréal QC H2Y 2X8
T: 514-871-8385
F: 514 871-8800
E: lex@tjl.quebec

Counsel for the Proposed Intervener, CCLA