AMERICAN BAR ASSOCIATION
International Law Section

INTERNATIONAL LAW NEWS

VOLUME 48 / ISSUE 3 / SPRING 2021

Privacy Compromised:
Searches of Electronic Devices at Ports of Entry

Sergio R. Karas and Zachary Gee

The increasing ubiquity and importance of electronic devices as part of our daily lives has produced a clash between individual privacy rights on one hand, and the protection of national security and investigation of criminal activity on the other. Nowhere is this clash more evident than for travelers crossing borders, where many constitutional protections are often weakened.

While basic protections apply at border crossings, immigration and customs agents have broad powers to search arriving travelers without a warrant. In recent years, searches of travelers' electronic devices, including phones, laptops, and tablets have become common. Information stored on the device may be reviewed and used to determine admissibility. The data contained in those devices can and has been used as the basis to lay criminal charges and obtain convictions. The ultimate question at the border is: Do warrantless searches of electronic devices at a port of entry violate constitutionally protected rights?

In 2006, the United States Ninth Circuit Court of Appeals opened the floodgates for electronic device searches at ports of entry with its decision in *U.S. v. Romm.*[1] The court held that a routine border search of the defendant's laptop was reasonable and that a warrant was not required. Later decisions confirmed that position. On the other hand, in Canada, the situation was murky, causing some confusion and concern about officers' powers to search electronic devices. With the increasing use of personal electronic devices, which are now ubiquitous, searches are occurring more often on both sides of the Canada-U.S. border.

The official guidelines for searches of arriving travelers by both the Canada Border Services Agency (CBSA) and the U.S. Customs and Border Protection (CBP) were issued in the form of directives in the -mid-2000s. They have not been completely overhauled to keep pace with technological advances. However, there is a growing body of jurisprudence that can inform on the scope of the powers that both CBSA and CBP officers can exercise when searching electronic devices. The Alberta Court of Appeal decision in *R. v. Canfield*[2] declared Section 99 of the Customs Act[3] unconstitutional and has shattered several decades of jurisprudence by calling into question the nature of electronic devices as "goods" and accepting that they have a significant role in our daily lives. The decision escalates the battle between privacy rights and criminal investigations.

Searches of electronic devices at Canadian ports of entry

When travelers arrive at a Canadian port of entry, Section 99 of the Customs Act grants CBSA Border Service Officers (BSOs) sweeping powers. The Ontario Superior Court of Justice classified electronic information on any device as a "good" entering the country in *R v. Moroz.*[4] All information on the device is treated like any other physical item in the traveler's luggage. This position is reflected in a broad CBSA policy statement regarding the examination of electronic devices:[5]

"CBSA officers do not always examine digital devices. Our policy is to examine a device only if we think we will find evidence on it that border laws have been broken. Reasons an officer might examine your digital device(s) include concerns regarding your:

- *admissibility or admissibility of your goods*
- *identity*
- *failure to comply with Canadian laws or regulations."*

The CBSA directive establishes that without a warrant, travelers are obligated to provide their device password in writing. Also, the device must be turned to airplane mode since data requiring internet access is out of the scope of the search. Anything on the hard drive of the device, including emails, is searchable. At the discretion of the CBSA officer, the device can be seized and detained if any semblance of suspicious or illegal activity is discovered. However, travelers have the option to

[1] 455 F (3d) 990 (9th Cir. 2006) [*Romm*].
[2] 2020 ABCA 383 [*Canfield*].
[3] RSC 1985, c 1.
[4] 2012 ONSC 5642.
[5] https://www.cbsa-asfc.gc.ca/travel-voyage/edd-ean-eng.html

challenge the search via an application to the CBSA Recourse Officer within ninety days and further appeal to the appropriate court. [6]

The CBSA directive contains a section dedicated to legal practitioners. Regarding solicitor-client privilege, it states that *"the CBSA is committed to respecting privacy rights while protecting the safety and security of the Canadian border. If a BSO encounters content marked as solicitor-client privilege, the officer must cease inspecting that document. If there are concerns about the legitimacy of solicitor-client privilege, the device can be set aside for a court to decide of the contents."* [7]

Canadian caselaw has addressed searches of arriving travelers at the border. In 1988, the Supreme Court of Canada (SCC) in *R v. Simmons*,[8] held that there are three main categories of border searches:

1) Routine questioning that every traveler undergoes at a port of entry, accompanied in some cases by a baggage search and perhaps a pat or frisk of outer clothing.[9] The SCC held that "*no stigma is attached to being one of the thousands of travelers who are daily routinely checked in that manner upon entry to Canada and no constitutional issues are raised. It would be absurd to suggest that a person in such circumstances is detained in a constitutional sense and therefore entitled to be advised of his or her right to counsel."*
2) *"Strip or skin search conducted in a private room, after a secondary examination and with the permission of a customs officer in authority."*
3) *"Body cavity search, in which customs officers have recourse to medical doctors, X-rays, emetics, and to other highly invasive means."* The court held that this is the most invasive type of search.[10]

Also, the Ontario Court of Appeal ruled in *R v. Jones*[11] that protecting the border is a principle of fundamental justice. Hence, the border presents a myriad of unique exceptions to the application of the *Charter of Rights and Freedoms*.[12] Officers enjoy broad powers and can search electronic devices almost at will.

Canadian courts have held that electronic devices fall under the first category described in *R v. Simmons* above. In *R v. Leask*[13] the Ontario Court of Justice ruled that a laptop computer is a good, one equivalent to any other physical good in the traveler's luggage. A few years later, in *R v. Moroz*,[14] the same court ruled that cell phones are also deemed a physical good.

The first category of searches in *R v. Simmons* is very broad and predates the advent of electronic devices. More recent Canadian caselaw has dealt directly with searches of electronic devices. In, *R v. Whittaker*,[15] the defendant, after being randomly selected for a secondary search, was suspected of entering Canada to work instead of vacation. A thorough search of his belongings was conducted, including one on two hard disk drives that he claimed to be the property of his employer. The search yielded images of child pornography, and he was charged and convicted of possession. He challenged the evidence, arguing that the search of the drives was unconstitutional and violated Section 8 of the *Charter*.[16] However, the New Brunswick Provincial Court ruled that a search of the stored contents of a laptop computer or external hard drive (memory stick) in the possession of a person seeking admission into Canada did not violate the rights guaranteed by Section 8."[17] *Whittaker* held that searches of electronic devices are considered nothing more than a regular search of goods, reasonable at a port of entry. The court held that since electronic devices contain pertinent information as to identity, reasons for entering, and physical goods of the traveler, the state has the right to inspect and control what enters the country.

R v. Buss[18] followed the reasoning set out in *R v. Whittaker.* In *Buss*, the legitimacy of travel by a U.S. citizen crossing the border raised suspicions. The defendant indicated that he was just planning to visit for 17 days, but that he was also planning to get married to a Canadian fiancée. Upon searching the defendant's phone, information contradicting his statements was found. The CBSA suspected that he intended to stay in Canada permanently. That led to a further search of his laptop, where child pornography was discovered. The defendant was charged and convicted of possession of child pornography. He appealed and argued that the search was unreasonable, since he had not been

[6] https://www.cbsa-asfc.gc.ca/recourse-recours/impartial-eng.html
[7] https://www.cbsa-asfc.gc.ca/travel-voyage/edd-ean-eng.html
[8] 1988 2 SCR 495.
[9] *Ibid*, at para 77.
[10] *Ibid* at para 27.
[11] 2006 ONCA 225.
[12] *The Constitution Act*, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11.
[13] 2008 ONCJ 25.
[14] 2012 ONSC 5642.
[15] 2010 NBPC 32 [*Whittaker*].
[16] *Supra* note 12, at s 8.
[17] *Whittaker, supra* note 15, at para 1.
[18] 2014 BCPC 16.

suspected of the crime at the time of the search, and thus his *Charter* rights were violated. The British Columbia Provincial Court ruled against the defendant and held that the border is a special zone. The court acknowledged that the *Charter* still applies, but that the state must protect national security and control its borders. *Buss* held that an initial suspicion at the border can lead to further searches unrelated to the original reason for suspicion. It must be noted, however, that most of the caselaw has been from lower courts, so it must be considered advisedly.

While travelers can challenge a warrantless search of electronic devices, they must do so at a court hearing within ninety days.[19] At that point, at least some information would have been already viewed and stored by CBSA compromising privacy. One item of particular interest to legal counsel is that in the absence of a clear assertion of solicitor-client privilege, officers are permitted to conduct a full search, and in the event of a dispute, the device is set aside for a court to determine what information can be examined.[20] CBSA officers have the discretion to determine the legitimacy of the assertion of the designation of a document as solicitor-client privileged, and hence, the power to search remains tipped in the CBSA's favor.

The decision by the Alberta Court of Appeal in *Canfield*[21] declared Section 99 (1)(a) of the *Customs Act* to be unconstitutional. In a lengthy decision, the court discussed the role of electronic devices in our lives and the invasive nature of searches of those devices at the port of entry. The facts of the case merit some discussion, as they appear to be rather unique.

Mr. Canfield and Mr. Townsend were each convicted of possession of child pornography. The evidence against them included photographs and videos retrieved when their electronic devices, which included a cell phone and laptop computer were searched at different times by CBSA at the Edmonton International Airport. Both appellants were Canadian citizens and were referred for secondary inspection upon re-entering Canada. Their electronic devices were searched. It is noteworthy that before the searches, both appellants made significant admissions as to the nature of their travel overseas, and that, coupled with their demeanor, raised some suspicion in the CBSA officers' minds. At trial, it was argued that the searches violated the appellants' constitutional rights to life, liberty, and the security of the person, and against unreasonable search and seizure, as protected by the *Charter of Rights and Freedoms*[22] and therefore the evidence found in the electronic devices was obtained illegally. Canfield and Townsend were convicted of possession of child pornography at trial. However, the Alberta Court of Appeal ruled:

> "For the reasons that follow, we are satisfied that the trial judge erred by failing to recognize that *Simmons* should be revisited to consider whether personal electronic devices can be routinely searched at the border, without engaging the *Charter* rights of those being searched. We have also concluded that s 99(1)(a) of the *Customs Act* is unconstitutional to the extent that it imposes no limits on the searches of such devices at the border, and is not saved by s 1 of the *Charter*. We accordingly declare that the definition of "goods" in s 2 of the *Customs Act* is of no force or effect insofar as the definition includes the contents of personal electronic devices for the purpose of s 99(1)(a). We suspend the declaration of invalidity for one year to provide Parliament the opportunity to amend the legislation to determine how to address searches of personal electronic devices at the border." [23]

The court held that the rights of the appellants were violated and that they were arbitrarily detained. However, the court allowed the evidence obtained from the electronic devices to be admitted supporting the convictions. The court held:

> "This is an evolving area of the law; there was nothing unreasonable in the reliance by the CBSA on the authority of *Simmons* and the jurisprudence following it. Quite the opposite; it would have been unreasonable not to rely on those authorities. The border officials acted in good faith in deciding to search the devices and in carrying out the searches. They uncovered real and reliable evidence of a serious offense that is crucial to the Crown's case."[24]

Canfield's application for leave to appeal was dismissed by the Supreme Court of Canada.[25]

[19] https://www.cbsa-asfc.gc.ca/recourse-recours/menu-eng.html.
[20] https://www.cbsa-asfc.gc.ca/travel-voyage/edd-ean-eng.html#04.
[21] *Canfield*, *supra* note 2.
[22] The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11, Sections 7, 8, and 10.
[23] *Canfield*, *supra* note 2 at para 7.
[24] *Ibid* at para 186.
[25] Leave to appeal to SCC dismissed, 2021 Canada Supreme Court Reports 39376.

Searches of electronic devices at U.S. ports of entry

Under 8 USC § 1357,[26] CBP is granted broad powers to search travelers without a warrant. Like CBSA, CBP has issued a directive regarding the search of electronic devices. The directive states that CBP strives to "protect rights against unreasonable search and seizure, ensure privacy protection while accomplishing enforcement of mission."[27]

Section 5.2 of the directive contains specific protections for attorney-client privileged information, to be followed officers become aware of the privilege. Officers may see some sensitive information before stopping that portion of the search.

In *Riley v. California*,[28] the United States Supreme Court ruled that a warrantless search of a cell phone during an arrest is unconstitutional. *Riley* prevents warrantless electronic searches inland, as the case did not involve the border of a port of entry. Searches at the border are covered under the "border search exception," as described in *U.S. v. Flores-Montano.*[29] This is an exception to the protection against unreasonable search and seizure afforded by the Fourth Amendment to the U.S. Constitution. [30]

U.S. v. Romm[31] held that the contents of a laptop computer may be searched at an international border without a warrant or probable cause. Notwithstanding the case law following *U.S. v. Romm*, *U.S. v. Cotterman*[32] added an interesting twist. A lengthy criminal record related to child sex tourism was used to justify additional screening of an arriving traveler, despite no immediate suspicion of illicit activity. A preliminary search of the defendant's electronics at the border found nothing but the device was nevertheless seized and shipped to a forensic lab. One hundred and seventy days later, images of child pornography were recovered from the device. The defendant was subsequently convicted of possession of child pornography. On appeal, he argued that the evidence should have been suppressed on the basis that there was no suspicion of child pornography that preceded the search and seizure. The Ninth Circuit Court of Appeals held that a traveler's personal property presented for inspection when entering the United States at the border may not be subject to forensic examination without a reason for suspicion. However, the Ninth Circuit also ruled that a track record of criminal activity combined with frequent questionable travel was enough to satisfy the test of reasonable suspicion.

A trio of 2018 cases have followed the decision in *Romm*. In *U.S. v. Vergara,*[33] the defendant was randomly selected for secondary screening, and a search of his electronic devices uncovered child pornography. While the defendant challenged the evidence in court, given that there was no suspicion of a crime at the time of the search, the Eleventh Circuit held that forensic searches can occur at the border without a warrant and are distinguishable from "searches classified as incident to arrest."[34] The court stated that border searches never require a warrant or probable cause but, at most, require reasonable suspicion".[35] Further, in *U.S. v. Touse*t,[36] the facts were similar to *Vergara.* CBP agents discovered that the defendant's name was flagged by a series of private investigations by internet service providers into unusual monetary transfers to countries involved in child sex tourism. CBP agents used that suspicion as the basis for a search of his electronic devices. The search yielded evidence of online child sex tourism and child pornography. The defendant was charged and convicted of receiving and possessing child pornography. The defendant appealed, arguing that the evidence should have been excluded because there was no initial reasonable suspicion of child pornography that preceded the search. However, the Eleventh Circuit affirmed that CBP can seize any electronic devices at the border and undertake comprehensive searches of those devices without any specific individualized suspicion of wrongdoing.[37]

Moreover, in *U.S. v. Kolsuz*,[38] the defendant was subjected to a search of his electronic devices after illegal firearms were found in his baggage during routine airport security screening. His phone was detained offsite, hundreds of miles from the border, for several

---

[26] *Aliens and Nationality*, 8 USC § 1357 (2006).
[27] https://www.cbp.gov/document/directives/cbp-directive-no-3340-049a-border-search-electronic-devices.
[28] 858 F (3d) 1012 (2014).
[29] 541 US 149 (9th Cir. 2004).
[30] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[31] *Romm, supra* note 1.
[32] 709 F (3d) 952 (9th Cir. 2013).
[33] 884 F(3d) 1309 (11th Cir. 2018).
[34] *Ibid*, at para 1.
[35] *Ibid.*
[36] 890 F (3d) 1227 (11th Cir 2018).
[37] *Ibid*, at 2.
[38] 890 F (3d) 133 (4th Cir. 2018).

months and subjected to a comprehensive search. It yielded a nine-hundred-page long report, which included content unrelated to firearms. Based on that evidence, the defendant was convicted of multiple offenses in addition to the firearms offense, including conspiracy to commit international smuggling. The defendant moved to suppress the evidence, arguing that the months-long detention of the phone offsite re-classified the search and detached it from the border exception. The Fourth Circuit Court of Appeals disagreed and allowed the conviction to stand. The court held that a mere reasonable suspicion at the border is sufficient to justify a search of all the content of a personal electronic device and that anything found from that time on, whether related to the original suspicion or not, is still covered by the border search exception.

Despite the trio of the above cases, *Cotterman* was followed and expanded in *Alasaad v. McAleenan*.[39] Nine arriving travelers to Boston's Logan International Airport, including U.S citizens, filed a class-action lawsuit after they were subjected to the search and seizure of their electronic devices. CBP had concerns about their prior travel history but had no specific suspicion of illegal activity. The searches yielded no evidence, yet their devices were detained for months. The plaintiffs claimed that it was a gross violation of their privacy rights. The U.S. District Court ruled in favor of the plaintiffs, holding that a warrantless search of an electronic device "without reasonable grounds of individualized suspicion of specific illegal activity was a violation of the Fourth Amendment."[40] The U.S. Court of Appeals for the First Circuit reversed this decision under the style of cause *Alasaad v. Mayorkas*.[41] The court held that there were no violations of the Fourth or First Amendments, and that advanced searches do not require a warrant or probable cause. The Court of Appeals held that the U.S. Supreme Court "has not specified the standard to assess alleged government intrusions on First Amendment rights at the border."[42] As for the Fourth Amendment, the court held that the border search exception applies to searches of electronic devices.

The First Circuit Court of Appeals recognized that its decision in *Alasaad* is at odds with that of the Ninth Circuit in *U.S. v. Cano.*[43] In that appeal, the panel reversed the District Court's order that denied the defendant's motion to supress evidence from the CBP warrantless search of his cell phone. The court held that the border search exception was "restricted in scope to searches for contraband."[44] Cano's conviction for importing cocaine was vacated. However, in *Alasaad*, the court cited *Riley* in holding that it would be more appropriate for Congress to identify threats of harm at the border. It held that "the border search exception is not limited to searches for contraband itself rather than evidence of contraband or a border-related crime."[45] A basic search involves the manual examination of a device. On the other hand, an advanced search requires reasonable suspicion and supervisory approval to connect external equipment to a device for review, copy, and/or analysis. The courts in *Alasaad* and *Cano* did agree that both types of border searches may be performed without probable cause or a warrant, and that basic border searches of electronic devices do not require reasonable suspicion.[46] The disagreement had to do with the scope of the search, which *Alasaad* extended beyond the mere search for contraband or evidence of a related crime.

On both sides of the Canada-U.S. border, travelers face a similar situation. Both CBSA and CBP have broad, sweeping powers to search and seize electronic devices without a warrant. While both agencies have shown willingness to protect attorney-client privilege, and safeguard privacy to the extent possible, the jurisprudence to date permits agents to search and seize electronic devices without a warrant at the slightest suspicion of a violation. It is advisable to store confidential data on remote cloud storage rather than on the device itself. For legal counsel, this is the best way to ensure the protection of solicitor-client privilege.

Sergio R. Karas, Karas Immigration Law Professional Corporation, is a Certified Specialist in Canadian Citizenship and Immigration Law by the Law Society of Ontario. He is Past Chair of the Ontario Bar Association Citizenship and Immigration Section, Past Chair of the International Bar Association Immigration and Nationality Committee, Past Chair of the Canada Committee, and current Co-Chair of the International Ethics Committee of the American Bar Association International Law Section. He is the Editor of the Global Business Immigration Handbook.

Zachary Gee is a JD candidate, 2022 at the University of Alberta, Faculty of Law. He holds a Bachelor of Commerce degree with Distinction from the University of Alberta with a major in Business Economics and Law.

[39] No. 17-cv-11730-DJC (Dist Mass. 2019).
[40] *Ibid*, at para 24.
[41] No. 20-1077 (1st Cir. 2021).
[42] *Ibid* at 27.
[43] 934 F (3d) 1002 (9th Cir. 2019).
[44] *Ibid* at 28.
[45] *Supra*, note 41, at 22.
[46] *Ibid* at 17; 19.