CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

CANADA BORDER SERVICES AGENCY

POLICY ON PORT OF ENTRY EXAMINATIONS OF TRAVELLERS' DIGITAL DEVICES

November 2019

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

POLICY STATEMENT **3**

DEFINITIONS **3**

PURPOSE AND SCOPE **3**

AUTHORITIES – CUSTOMS ACT / IRPA **5**

ROLES AND RESPONSIBILITIES **11**

ROLE OF BORDER SERVICES OFFICERS 11
ROLE OF INTELLIGENCE OFFICERS 11
ROLE OF SUPERINTENDENTS 12
ROLE OF CHIEFS 12

POLICIES AND PROCEDURES **13**

WHEN A TRAVELLER'S DIGITAL DEVICE CAN BE EXAMINED 13
NOTE TAKING 15
WHAT CAN BE EXAMINED 17
PRIVACY AND PRESENCE OF TRAVELLER 18
DEVICE PASSWORDS AND SECURITY 19
DISABLING NETWORK CONNECTIVITY 20
HOW A DEVICE SHOULD BE EXAMINED 21
COPYING/REPRODUCING DATA FROM A TRAVELLER'S DIGITAL DEVICE 22
REPORTING OF DIGITAL DEVICE EXAMINATION 23
ENCOUNTERING INTIMATE IMAGES AND OTHER SENSITIVE MATERIAL 23
..... 24
SOLICITOR-CLIENT PRIVILEGED INFORMATION AND JUDICIAL INFORMATION 25
ENCOUNTERING EVIDENCE OF A CRIMINAL NATURE 26
DIGITAL DEVICE EXAMINATIONS AND LOOKOUT PROCEDURES 27

DETENTION AND SEIZURE OF DEVICE **28**

REFUSAL TO PROVIDE MEANS OF ACCESSING A DIGITAL DEVICE **28**

SHARING OF INFORMATION OR DATA DISCOVERED ON A TRAVELLER'S DIGITAL DEVICE **30**

ACCOMPANYING RESOURCES **30**

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Policy Statement

1. Digital devices, media, documents, software and stored electronic data are considered "goods" under Canada Border Services Agency (CBSA) program legislation and are subject to examination by CBSA Officers at ports of entry/customs offices (hereafter "ports of entry") for the administration and enforcement of CBSA program legislation. Examinations of digital devices and media can facilitate informed decision-making regarding admissibility and entry of people and goods to Canada under CBSA program legislation. CBSA Officers carrying out examinations of travellers' digital goods shall adhere to this policy.
2. Though digital devices are considered goods and can be examined as such, as a matter of policy, examinations of digital devices should not be conducted as a matter of course.

Definitions

3. "Digital device" for the purposes of this policy means mobile phones (cell phones), smartphones, computers, tablets, removable media, drives, cameras, smartwatches, and any other device capable of storing digital data in the actual possession or accompanying baggage of the traveller.
4. If a CBSA Officer is unsure as to whether a digital device is capable of storing digital data the Officer must include the device within the definition of digital device.
5. "CBSA program legislation" is defined in section 2 of the *Canada Border Services Agency Act*.

Purpose and Scope

6. The purpose of this policy is to provide CBSA Officers with a framework for the lawful, reasonable and progressive port of entry examinations of travellers' digital devices while

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

recognizing and respecting the potential private nature of information contained within these devices[1].

7. CBSA Officers, as with other non-digital information encountered, are bound to maintain the confidentiality of this information, except where sharing is permitted by law.
8. This policy applies to any CBSA Officer[2] who may, as part of their duties, examine a traveller's digital device as part of a secondary examination under the *Customs Act* or the *Immigration and Refugee Protection Act* (IRPA) at a port of entry.
9. This policy applies to inbound, port of entry examinations of travellers' digital devices.
10. This policy does not apply to commercial quantities of digital devices, or digital devices imported for commercial purposes.
11. This policy does not apply to examinations performed under section 99.3 of the *Customs Act* (see Enforcement Manual Part 6, Chapter 9 – Customs Controlled Areas).
12. This policy does not apply to instances where a traveller's digital device is examined or searched:
    a. to determine if physical (i.e. non-digital) contraband is contained within or on the device itself (ex: contraband hidden in a cavity within a device);
    b. under judicial authorization (i.e. search warrant);
    c. incident to arrest;
    d. in relation to *IRPA* A16(1) or A16(3), when applied outside of the port of entry context (e.g. overseas or within Canada);
    e. solely to determine if the digital device functions; or

[1] In a criminal investigative inland context, Canadian courts have recognized that digital devices can have unique characteristics that differentiate them from other items subject to a search

[2] The CBSA employee must meet the definition of "officer" under the relevant provisions of the *Customs Act* and the *IRPA* to conduct these examinations under both the *Customs Act* and the *IRPA*

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

f. when a traveller displays digital content to an Officer, in an attempt to demonstrate compliance with CBSA program legislation or to provide additional context or information relevant to their admissibility or compliance (ex: a digital copy of a work or study permit, or receipts to show the value of an item), provided the viewing of that content by the Officer does not progress to a more detailed examination of the device's contents not initially displayed to the Officer.

Note: When the above 11. f) circumstances are met, CBSA Officers must still ensure that any subsequent obtaining of information from the interaction is within the scope of lawful authority and is for valid CBSA program legislation purposes.

13. This policy does not limit any examination authority conferred on any CBSA Officer under any Act of Parliament.

Authorities – Customs Act / IRPA

14. The *Customs Act* and IRPA authorities to examine digital devices by CBSA Officers at the border can remain available throughout an interaction with a traveller until the examination or assessment is completed. Possible concerns such as identity, admissibility of persons, smuggling and/or release of goods can occur simultaneously.

    Note: CBSA Officers must be mindful of distinctions as between CBSA's relevant authorities (eg.: IRPA 16(3) does not apply to Canadian citizens whereas IRPA 139 requires reasonable grounds to believe)."

15. If a digital device examination is performed simultaneously for non-compliance under both the *Customs Act* and the *IRPA,* the examining Officer must adhere simultaneously to the specific legislative criteria under the specific legislative examination authorities on which the

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Officer is relying to conduct the digital device examination at the port of entry, as well as this policy.

16. If a digital device examination progresses to require further exercise of CBSA authorities (eg.: obtaining, detaining, seizing, etc.), the relevant officer must continue to adhere to the specific legislative authority's requirements and associated CBSA policy guidance appropriate to the circumstances.

Customs Act – Obligations of Travellers

17. Section 7.1 of the *Customs Act* states: "Any information provided to an officer in the administration or enforcement of this Act, the *Customs Tariff* or the *Special Import Measures Act* or under any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, shall be true, accurate and complete."
18. Section 11 (1) of the *Customs Act* states: "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present [themselves]to an officer and answer truthfully any questions asked by the officer in the performance of [their] duties under this or any other Act of Parliament."
19. Section 12 (1) of the *Customs Act* states: "all goods that are imported shall, except in such circumstances and subject to such conditions as may be prescribed, be reported at the nearest customs office designated for that purpose that is open for business."
20. Section 13 of the *Customs Act* states: "Every person who reports goods under section 12 inside or outside Canada or is stopped by an officer in accordance with section 99.1 shall

(a) answer truthfully any question asked by an officer with respect to the goods; and

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

(b) if an officer so requests, present the goods to the officer, remove any covering from the goods, unload any conveyance or open any part of the conveyance, or open or unpack any package or container that the officer wishes to examine."

***Customs Act* - Examination of Goods Authorities**

21. Section 99 (1) (a) of the *Customs Act* allows an officer: "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;"
22. Section 99 (1) (e) of the *Customs Act* states: "where the officer suspects on reasonable grounds that this Act or the regulations or any other Act of Parliament administered or enforced by [them] or any regulations thereunder have been or might be contravened in respect of any goods, examine the goods and open or cause to be opened any package or container thereof;"

***Customs Act* – Detention of Goods Authority**

23. Section 101 of the *Customs Act* states: "goods that have been imported or are about to be exported may be detained by an officer until [they are] satisfied that the goods have been dealt with in accordance with this Act, and any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, and any regulations made thereunder."

***Customs Act* – Seizure of Goods Authority**

24. Section 110 (1) (a) of the *Customs Act* states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened in respect of goods, seize as forfeit

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

a. The goods;"

25. Section 110 (3) states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened, seize anything that [they believe] on reasonable grounds will afford evidence in respect of the contravention."

Customs Act* – *Copying Authority

26. Section 115(1) states: "If any record is examined or seized under this Act, the Minister, or the officer by whom it is examined or seized, may make or cause to be made one or more copies of it, and a copy purporting to be certified by the Minister or a person authorized by the Minister is admissible in evidence and has the same probative force as the original would have if it had been proved in the ordinary way."

***Criminal Code* – Seizure without warrant**

27. Section 489 (2) of the Criminal Code states: "Every peace officer, and every public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, who is lawfully present in a place pursuant to a warrant or otherwise in the execution of duties, may, without a warrant, seize any thing that the officer believes on reasonable grounds

    a. has been obtained by the commission of an offence against this or any other Act of Parliament;
    b. has been used in the commission of an offence against this or any other Act of Parliament; or
    c. will afford evidence in respect of an offence against this or any other Act of Parliament.

Immigration and Refugee Protection Act (IRPA) – obligations of persons seeking entry

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

28. Section 16 (1) of the *IRPA* states: "A person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires."
29. Section 16 (1.1) states: "A person who makes an application must, on request of an officer, appear for an examination."
30. Section 16 (2) states: "In the case of a foreign national,
    a. The relevant evidence referred to in subsection (1) includes photographic and fingerprint evidence; and
    b. Subject to the regulations, the foreign national must submit to a medical examination."
31. Section 18 (1) of *IRPA* states: "Subject to the regulations, every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

Immigration and Refugee Protection Act (IRPA) – examination authorities

32. Section 15 (1) of the *IRPA* states: "An officer is authorized to proceed with an examination if a person makes an application to the officer in accordance with this Act or if an application is made under subsection 11(1.01)."[3]
33. Section 15 (3) of the *IRPA* states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies of extracts and hold the means of transportation until the inspection and examination are completed."

[3] Section 11 (1.01) of the *IRPA* addresses mandatory electronic travel authorizations made by foreign nationals prior to entry.

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

34. Section 16 (3) of the *IRPA* states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."
35. Section 139 of the *IRPA* states: "An officer may search any person seeking to come into Canada and may search their luggage and personal effects and the means of transportation that conveyed the person to Canada if the officer believes on reasonable grounds that the person
    a. has not revealed their identity or has hidden on or about their person documents that are relevant to their admissibility; or
    b. has committed, or possess documents that may be used in the commission of, an offence referred to in section 117, 118, or 122."

***Immigration and Refugee Protection Act* – seizure authority**

36. Section 140 (1) of the *IRPA* states: "An officer may seize and hold any means of transportation, document or other thing if the officer believes on reasonable grounds that it was fraudulently or improperly obtained or used or that the seizure is necessary to prevent its fraudulent or improper use or to carry out the purposes of this Act."

Immigration and Refugee Protection Act – Copying Authorities

37. Section 15(3) of the IRPA states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies or extracts and hold the means of transportation until the inspection and examination are completed."

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

38. Section 16(3) of the IRPA states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."

Roles and Responsibilities

Role of Border Services Officers

39. BSOs working at ports of entry must be familiar with the policy on the examination of travellers' digital devices.
40. BSOs are responsible for taking the mandatory training on the Examination of Digital Devices
41. BSOs are responsible for adhering to this policy on the examination of travellers' digital devices.
42. As per the policy guidance contained herein, BSOs are responsible for:
    a. remaining sensitive to the potential private nature of data stored on digital devices;
    b. following guidance on when and how digital devices can be examined;
    c. reporting any examinations of travellers' digital devices to CBSA Headquarters; and
    d. making accurate, contemporaneous and detailed notes whenever a traveller's digital device is examined.

Role of Intelligence Officers

43. Intelligence Officers are responsible for:

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

a. Familiarizing themselves with the policy on examinations of travellers' digital devices, and
b. Remaining available to consult with other CBSA Officers who may examine travellers' digital devices, including BSOs that encounter lookouts when processing travellers, to provide additional information to the BSO that could assist the BSO in determining if a digital device examination is justified.

Role of Superintendents

44. Superintendents are responsible for:

a. Familiarizing themselves with the policy on examinations of travellers' digital devices;
b. Ensuring BSOs working in the traveller continuum familiarize themselves with the policy on examinations of travellers' digital devices; and
c. Ensuring BSOs follow the policy guidance contained herein, including but not limited to:
    i. Not conducting digital device exams as a matter of course;
    ii. Taking accurate, contemporaneous and detailed notes when devices are examined;
    iii. Remaining sensitive to the potential private nature of these goods; and
    iv. Reporting to CBSA HQ all instances of examinations of travellers' digital devices.
d. Performing periodic compliance verifications to ensure BSOs are following the policies contained herein.

Role of Chiefs

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

45. Chiefs are responsible for:
    a. Ensuring ports of entry in their jurisdiction are aware of the policy on examinations of travellers' digital devices;
    b. Ensuring BSOs in their jurisdiction have completed the requisite training on the examination of digital devices;
    c. Ensuring Superintendents exercise due diligence in reporting instances of digital device examinations to CBSA Headquarters; and
    d. Ensuring Superintendents perform periodic compliance verifications to ensure BSOs are following the policies contained herein, including note taking.

Policies and Procedures

When a Traveller's Digital Device Can Be Examined

46. Examinations of travellers' digital devices must be performed with a clear link to administering or enforcing CBSA program legislation that governs the cross-border movement of people and goods, including animals and plants.
47. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence under any Act of Parliament.
48. See the section on Encountering Evidence of a Criminal Nature in this policy for further instruction.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Acces a l'informat

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Notetaking

53. Accurate, contemporaneous and detailed record-keeping in officer notebooks is essential when conducting examinations of travellers' digital devices.
54. These note taking requirements must be followed even in the instance that the examination of a traveller's digital device is non-resultant.
55. The note taking directives described herein consider the Supreme Court of Canada jurisprudence in inland contexts in relation to the obligation to keep a careful record when conducting a search of a digital device in the absence either of judicial authorization or reasonable and probable grounds. The note taking directives aim to protect CBSA Officers and support CBSA's legal authorities. Courts have also recognized that the record-keeping requirement will have the incidental effect of helping Officers focus on the question of whether their conduct in relation to the examination of the device falls squarely within the parameters of a lawful examination for CBSA program legislation purposes.

56. Accurate, contemporaneous and detailed note taking will:
    a. Assist Officers in being able to articulate each step of a CBSA port of entry digital device examination for the purposes of CBSA program legislation;
    b. Serve as evidence should legal proceedings ensue;
    c. Protect the officer and the CBSA should allegations of misconduct arise through internal CBSA complaint mechanisms or external review or complaint bodies; and

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

d. Serve as a record of the judicious and lawful use of the statutory authorities available to officers.

57. The note taking directives contained herein are in addition to the note taking requirements identified in the agency's Notebook Policy, found in Part 8, Chapter 1 of the Enforcement Manual.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information.

59. Any information examined residing on a traveller's digital device must be linked to relevant legislated CBSA program concerns[5] and the examination must take place within the scope of an applicable lawful authority.

60. Section 16 (3) of the *IRPA* authorizes an Officer to require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence that may be used to establish their identity or compliance with the *IRPA*. Where an Officer has concerns regarding identity or non-compliance with the *IRPA*, they may examine relevant data on the permanent resident or foreign national's digital device, as reasonably required, to determine identity or non-compliance under the *IRPA*.

61. Sections 34 through 42 of the *IRPA* set out the conditions under which a foreign national or permanent resident is inadmissible to Canada. Where an Officer has concerns that an individual may be inadmissible, they may examine relevant data on the traveller's digital device, as reasonably required, to determine admissibility.

[5] CBSA program legislation is defined in section 2 of the *Canada Border Service Agency Act*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

62. In terms of importation, under section 99 (1) (a) of the *Customs Act* only goods that have been imported are subject to examination by CBSA Officers, up until the time of release.
63. Therefore, CBSA Officers are only authorized by section 99 (1) (a) of the *Customs Act* to examine data that resides on a digital device at the time of importation, at any time up to the time of release.
64. To avoid mistakenly examining data not residing on the device at the time of importation, officers should take steps to disable network connectivity before the examination begins: See the Disabling Network Connectivity section below.

Privacy and Presence of Traveller

65. CBSA Officers must remain cognisant of the potential private nature of data stored on travellers' devices, remain sensitive, discreet and professional to minimize potential embarrassment to travellers.
66. Digital devices and media may hold data related to, for example, personal photos, journal entries, text messages, group chats, travel history, intimate imagery, medical information and medical history (see the Encountering intimate images and other sensitive material section), legal advice (see the Solicitor-Client privileged and Judicial information section), financial information, and other private details.
67. Where operationally feasible, Officers should perform examinations of travellers' digital devices in the presence of the traveller to mitigate against potential concerns of the traveller.
68. When a traveller is present for the examination, Officers should be prepared to explain:
    a. the authority under which they are conducting the examination;
    b. the rationale(s) for the examination, if appropriate; and

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

c. that no information will be seized or any data copied unless required as evidence of a contravention or offence.

Device Passwords and Security

69. Digital devices are frequently protected with a password or other security method (e.g. passcode, biometrics, etc.). In order for an Officer to examine a digital device a traveller must supply the means for the device to be examined.
70. Where a password is required to gain access to a digital device, Officers should explain to a traveller that a password must be supplied in order for the traveller's obligations on entry to Canada under the *Customs* Act, the *IRPA* or other CBSA program legislation to be fulfilled.
71. While a device may primarily be protected by a biometrics-enabled method, the device can often also be accessed through a password. Where possible, Officers should seek to gain access to devices using this latter type of security method.

73. Officers should notate a device's password on a separate piece of paper in order to ensure it can be accessed at a later date, should prohibited content or evidence be found (see the Note taking directives section for more information).
74. If the examination is resultant, Officers should copy the password from the separate piece of paper into their officer notebook.
75. If the examination of a digital device is non-resultant, Officers should not retain the password or passcode. Officers should provide the traveller with the piece of paper upon which they recorded the password or passcode. Officers should record that they have done so in their officer notebook.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

76. Officers shall inform the traveller that their password or passcode, if retained, will be protected in accordance with privacy legislation.
77. After a non-resultant examination, Officers shall inform the traveller that their password or passcode can be changed immediately.
78. Officers should not record passwords to travellers' digital devices in CBSA systems, including the Integrated Customs Enforcement System (ICES) or the Integrated Customs System (ICS).

    Note: Officers should continue to use standard operating procedures to submit passwords to the Prohibited Importations Unit.

Disabling Network Connectivity

79. CBSA Officers must only access data that is stored on a traveller's digital device and must not access **any data** stored remotely.
80. In order to prevent accessing remote data, Officers should, before beginning the examination, deactivate its network connectivity.
81. Officers should note the if they were able to deactivate network connectivity in their notebooks.
82. Deactivating network connectivity can also prevent remote wiping or locking.
83. Activating "airplane mode" **may not disable all** network connectivity. Officers must ensure that the device is not connected to a WiFi network, wirelessly tethered to another device, or is sharing a connection with another device via Bluetooth.
84. Normally the status of network connectivity is indicated by icons in the top of the screen. If unsure, an Officer may choose to open the settings of the device and verify connectivity.
85. Officers may also ask the traveller how to disable network connectivity, however, the traveller should not perform this function themselves.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

How a Device Should be Examined

86. Enforcement Manual Part 4, Chapter 3 addresses how Officers should conduct personal baggage, goods and conveyance examinations. This policy on port of entry examinations of travellers' digital devices offers further precision in respect of examining travellers' digital goods but should be read in conjunction with that chapter of the manual.
87. Enforcement Manual Part 4, Chapter 3 stipulates that all examinations by Officers must be conducted in strict adherence to the CBSA's core values. Examinations must be proficient and discrete to the extent possible with respect to travellers and their goods, and all examinations must be conducted in a courteous and professional manner in accordance with the CBSA *Code of Conduct*.
88. Just as secondary examinations should be methodical, progressive and responsive as new indicators or information is discovered by or revealed to the Officer, so should any secondary examination of a traveller's digital device.
89. An examination of a traveller's digital device should be tailored to the purposes of the CBSA program legislation and should not be conducted as a matter of course.
90. In order to expedite the examination and if practical, an Officer may ask the traveller to point to the relevant area of the device for which the Officer has CBSA border screening and processing concerns. Focussing the examination will maximize efficiency for the Officer and minimize inconvenience to the traveller.
91. As a matter of policy, a port of entry digital device examination should be limited to:
    a. the examination of content for concerns related to CBSA program legislation; and
    b. areas of the device and data directly related to indicators or concerns identified by the Officer during the interaction with the traveller.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

92. Officers should be able to clearly articulate their reasoning for examining each type of data on the device, its link to indicators or concerns identified by the Officer, and the data's anticipated relevance to CBSA program legislation.
93. If, during the examination, additional indicators of concern are observed, the examination may expand and progress beyond the Officer's initial intent, provided diligent notes are taken regarding how and why the examination progresses.
94. Port of entry examinations should only be conducted manually and without the assistance of software/hardware.

Copying/Reproducing Data From a Traveller's Digital Device

95. Officers shall advise the traveller that their information will be protected by CBSA in accordance with applicable law including the *Privacy Act* and the *Customs Act*.
96. Officers shall not make copies of, duplicate or reproduce data examined on digital devices, including taking photographs or screenshots, unless such copying is authorized in the circumstances under CBSA program legislation and required for the specific and direct administration or enforcement of CBSA program legislation.
97. Officers shall not notate in their notebook or record in a CBSA system personal any information including contacts, phone numbers, names, dates of birth or other information from devices unless such notating or recording is authorized in the circumstances under CBSA program legislation, and required for the specific and direct administration or enforcement of CBSA program legislation.
98. Officers may rely on their regulatory copying authorities appropriate to the circumstances (*Customs Act* 115(1), IRPA 15(3) or 16(3)) if the legislative criteria in the relevant authority are met, and, only if the copying is for the specific and direct regulatory administration or enforcement of CBSA program legislation. In these cases, travellers are to be informed that

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

their information has been copied and that their information will be protected by the CBSA in accordance with applicable law including the *Privacy Act* and *Customs Act.*

99. Officers must use a CBSA-issued camera for any copying and must note the timestamp on the photograph in their notebook.

Reporting of Digital Device Examination

101. Effective November 2017, all examinations of travellers' digital devices must be reported to CBSA Headquarters as per Operational Bulletin 2017-61.

102. It is the policy of the CBSA to nationally track:

   a. the number of examinations of travellers' digital devices;

   b. the date of the examinations; and

   c. the port of entry at which the examinations took place.

103. CBSA Officers are expected to record in their notebooks all other information pertaining to digital device exams as per the Note taking directives section (e.g. the indicators that led to the digital device examination, the areas of the device accessed, etc.).

Encountering Intimate Images and Other Sensitive Material

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

104. A traveller may be particularly concerned if intimate images[6] of themselves or others are saved on the device.

105. If a traveller alerts an Officer to the presence of intimate images of themselves or others, the Officer should ask the traveller if there is a way to reasonably circumvent the viewing of those images.

[6] Intimate image is defined in s. 162.1 (2) of the *Criminal Code*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

119. If an Officer believes that the examination would compromise the solicitor-client privilege or judicial information, the Officer should:

    a. Notify and consult with their immediate supervisor with respect to the circumstances; and
    b. Determine with the supervisor if the device should be released, or
    c. Detain (*Customs* Act 101) or seize (IRPA 140(1)) the device without being examined, seal the device in a package marked with the assumption they are privileged, and set the device aside for review by a court or analogous independent review body for confirmation of privilege.

120. Officers can contact their region's Justice Liaison Officer for information on how to proceed with confirmation of privilege.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

125. In these circumstances, officers must also be cognisant that continuing the examination could potentially alter digital evidence (e.g. timestamps indicating when the file was last accessed).

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Detention and seizure of device

129. Part 5, Chapters 2 and 3 of the Enforcement Manual are the primary guidance documents for the seizure of evidence and goods from travellers.

Refusal to provide means of accessing a digital device

130. During a border examination upon entry to Canada, travellers have the legal obligation under the *Customs Act* to provide the means to access their goods, including digital devices, as well as the obligation to produce all relevant evidence that an Officer reasonably requires under the *IRPA*.

131. Every reasonable opportunity should be given to the traveller to fulfill their obligations at the port of entry under CBSA program legislation in providing the means to access their digital device.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

133. During the course of a regulatory examination of a traveller's digital device at secondary, assistance to gain access to the device shall not be obtained from any source outside the CBSA.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Sharing of information or data discovered on a traveller's digital device

139. The CBSA's primary guidance document on disclosure of "customs information," as defined in Section 107 of the ***Customs Act,*** is the Policy on the Disclosure of Customs Information: Section 107 of the *Customs Act*. This document should guide CBSA Officers when determining if they may provide access to customs information, in any form (e.g. hard copy, electronic or video format).

140. If information collected during a secondary examination does not meet the definition of "customs information" but instead meets the definition of "personal information" as defined in the *Privacy Act,* CBSA Officers should consult the Policy on the Disclosure of Personal Information: Section 8 of the *Privacy Act* for guidance.

Accompanying Resources

141. This policy document is not intended to be a standalone document, and should be read in conjunction with the following resources:

Canada Border Services Agency Act
Customs Act
Immigration and Refugee Protection Act
Privacy Act
Criminal Code
Canada Border Services Agency Code of Conduct
Canada Border Services Agency Enforcement Manual

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Enforcement Manual
Operational Bulletins
Shift Briefing Bulletins
Training and Learning products

Please note: This is not an exhaustive list of resources; the list will be updated as policy changes are made.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

ENFORCEMENT MANUAL

Part 4

EXAMINATION – GOODS AND CONVEYANCES

Chapter 16

POLICY ON PORT OF ENTRY EXAMINATIONS OF TRAVELLERS' DIGITAL DEVICES

April 2021

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

POLICY STATEMENT **3**

DEFINITIONS **3**

PURPOSE AND SCOPE **3**

AUTHORITIES – CUSTOMS ACT / IRPA **5**

ROLES AND RESPONSIBILITIES **11**

ROLE OF BORDER SERVICES OFFICERS 11
ROLE OF INTELLIGENCE OFFICERS 11
ROLE OF SUPERINTENDENTS 12
ROLE OF CHIEFS 12

POLICIES AND PROCEDURES **13**

WHEN A TRAVELLER'S DIGITAL DEVICE CAN BE EXAMINED 13
NOTE TAKING 15
WHAT CAN BE EXAMINED 17
PRIVACY AND PRESENCE OF TRAVELLER 18
DEVICE PASSWORDS AND SECURITY 19
DISABLING NETWORK CONNECTIVITY 20
HOW A DEVICE SHOULD BE EXAMINED 21
COPYING/REPRODUCING DATA FROM A TRAVELLER'S DIGITAL DEVICE 22
REPORTING OF DIGITAL DEVICE EXAMINATION 23
ENCOUNTERING INTIMATE IMAGES AND OTHER SENSITIVE MATERIAL 23
..... 24
SOLICITOR-CLIENT PRIVILEGED INFORMATION AND JUDICIAL INFORMATION 25
ENCOUNTERING EVIDENCE OF A CRIMINAL NATURE 26
DIGITAL DEVICE EXAMINATIONS AND LOOKOUT PROCEDURES 27

DETENTION AND SEIZURE OF DEVICE **28**

REFUSAL TO PROVIDE MEANS OF ACCESSING A DIGITAL DEVICE **28**

SHARING OF INFORMATION OR DATA DISCOVERED ON A TRAVELLER'S DIGITAL DEVICE **30**

ACCOMPANYING RESOURCES **30**

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Policy Statement

1. Digital devices, media, documents, software and stored electronic data are considered "goods" under Canada Border Services Agency (CBSA) program legislation and are subject to examination by CBSA Officers at ports of entry/customs offices (hereafter "ports of entry") for the administration and enforcement of CBSA program legislation. Examinations of digital devices and media can facilitate informed decision-making regarding admissibility and entry of people and goods to Canada under CBSA program legislation. CBSA Officers carrying out examinations of travellers' digital goods shall adhere to this policy.
2. Though digital devices are considered goods and can be examined as such, as a matter of policy, examinations of digital devices should not be conducted as a matter of course.

Definitions

3. "Digital device" for the purposes of this policy means mobile phones (cell phones), smartphones, computers, tablets, removable media, drives, cameras, smartwatches, and any other device capable of storing digital data in the actual possession or accompanying baggage of the traveller.
4. If a CBSA Officer is unsure as to whether a digital device is capable of storing digital data the Officer must include the device within the definition of digital device.
5. "CBSA program legislation" is defined in section 2 of the *Canada Border Services Agency Act*.

Purpose and Scope

6. The purpose of this policy is to provide CBSA Officers with a framework for the lawful, reasonable and progressive port of entry examinations of travellers' digital devices while

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

recognizing and respecting the potential private nature of information contained within these devices[1].

7. CBSA Officers, as with other non-digital information encountered, are bound to maintain the confidentiality of this information, except where sharing is permitted by law.
8. This policy applies to any CBSA Officer[2] who may, as part of their duties, examine a traveller's digital device as part of a secondary examination under the *Customs Act* or the *Immigration and Refugee Protection Act* (IRPA) at a port of entry.
9. This policy applies to inbound, port of entry examinations of travellers' digital devices.
10. This policy does not apply to commercial quantities of digital devices, or digital devices imported for commercial purposes.
11. This policy does not apply to examinations performed under section 99.3 of the *Customs Act* (see Enforcement Manual Part 6, Chapter 9 – Customs Controlled Areas).
12. This policy does not apply to instances where a traveller's digital device is examined or searched:
    a. to determine if physical (i.e. non-digital) contraband is contained within or on the device itself (ex: contraband hidden in a cavity within a device);
    b. under judicial authorization (i.e. search warrant);
    c. incident to arrest;
    d. in relation to *IRPA* A16(1) or A16(3), when applied outside of the port of entry context (e.g. overseas or within Canada);
    e. solely to determine if the digital device functions; or

[1] In a criminal investigative inland context, Canadian courts have recognized that digital devices can have unique characteristics that differentiate them from other items subject to a search

[2] The CBSA employee must meet the definition of "officer" under the relevant provisions of the *Customs Act* and the *IRPA* to conduct these examinations under both the *Customs Act* and the *IRPA*

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

f. when a traveller displays digital content to an Officer, in an attempt to demonstrate compliance with CBSA program legislation or to provide additional context or information relevant to their admissibility or compliance (ex: a digital copy of a work or study permit, or receipts to show the value of an item), provided the viewing of that content by the Officer does not progress to a more detailed examination of the device's contents not initially displayed to the Officer.

Note: When the above 11. f) circumstances are met, CBSA Officers must still ensure that any subsequent obtaining of information from the interaction is within the scope of lawful authority and is for valid CBSA program legislation purposes.

13. This policy does not limit any examination authority conferred on any CBSA Officer under any Act of Parliament.

Authorities – Customs Act / IRPA

14. The *Customs Act* and IRPA authorities to examine digital devices by CBSA Officers at the border can remain available throughout an interaction with a traveller until the examination or assessment is completed. Possible concerns such as identity, admissibility of persons, smuggling and/or release of goods can occur simultaneously.

    Note: CBSA Officers must be mindful of distinctions as between CBSA's relevant authorities (eg.: IRPA 16(3) does not apply to Canadian citizens whereas IRPA 139 requires reasonable grounds to believe)."

15. If a digital device examination is performed simultaneously for non-compliance under both the *Customs Act* and the *IRPA,* the examining Officer must adhere simultaneously to the specific legislative criteria under the specific legislative examination authorities on which the

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Officer is relying to conduct the digital device examination at the port of entry, as well as this policy.

16. If a digital device examination progresses to require further exercise of CBSA authorities (eg.: obtaining, detaining, seizing, etc.), the relevant officer must continue to adhere to the specific legislative authority's requirements and associated CBSA policy guidance appropriate to the circumstances.

Customs Act – Obligations of Travellers

17. Section 7.1 of the *Customs Act* states: "Any information provided to an officer in the administration or enforcement of this Act, the *Customs Tariff* or the *Special Import Measures Act* or under any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, shall be true, accurate and complete."
18. Section 11 (1) of the *Customs Act* states: "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present [themselves]to an officer and answer truthfully any questions asked by the officer in the performance of [their] duties under this or any other Act of Parliament."
19. Section 12 (1) of the *Customs Act* states: "all goods that are imported shall, except in such circumstances and subject to such conditions as may be prescribed, be reported at the nearest customs office designated for that purpose that is open for business."
20. Section 13 of the *Customs Act* states: "Every person who reports goods under section 12 inside or outside Canada or is stopped by an officer in accordance with section 99.1 shall

    (a) answer truthfully any question asked by an officer with respect to the goods; and

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

(b) if an officer so requests, present the goods to the officer, remove any covering from the goods, unload any conveyance or open any part of the conveyance, or open or unpack any package or container that the officer wishes to examine."

***Customs Act* - Examination of Goods Authorities**

21. Section 99 (1) (a) of the *Customs Act* allows an officer: "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;"
22. Section 99 (1) (e) of the *Customs Act* states: "where the officer suspects on reasonable grounds that this Act or the regulations or any other Act of Parliament administered or enforced by [them] or any regulations thereunder have been or might be contravened in respect of any goods, examine the goods and open or cause to be opened any package or container thereof;"

***Customs Act* – Detention of Goods Authority**

23. Section 101 of the *Customs Act* states: "goods that have been imported or are about to be exported may be detained by an officer until [they are] satisfied that the goods have been dealt with in accordance with this Act, and any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, and any regulations made thereunder."

***Customs Act* – Seizure of Goods Authority**

24. Section 110 (1) (a) of the *Customs Act* states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened in respect of goods, seize as forfeit

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

a. The goods;"

25. Section 110 (3) states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened, seize anything that [they believe] on reasonable grounds will afford evidence in respect of the contravention."

Customs Act – Copying Authority

26. Section 115(1) states: "If any record is examined or seized under this Act, the Minister, or the officer by whom it is examined or seized, may make or cause to be made one or more copies of it, and a copy purporting to be certified by the Minister or a person authorized by the Minister is admissible in evidence and has the same probative force as the original would have if it had been proved in the ordinary way."

***Criminal Code* – Seizure without warrant**

27. Section 489 (2) of the Criminal Code states: "Every peace officer, and every public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, who is lawfully present in a place pursuant to a warrant or otherwise in the execution of duties, may, without a warrant, seize any thing that the officer believes on reasonable grounds

    a. has been obtained by the commission of an offence against this or any other Act of Parliament;

    b. has been used in the commission of an offence against this or any other Act of Parliament; or

    c. will afford evidence in respect of an offence against this or any other Act of Parliament.

Immigration and Refugee Protection Act (IRPA) – obligations of persons seeking entry

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

28. Section 16 (1) of the *IRPA* states: "A person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires."
29. Section 16 (1.1) states: "A person who makes an application must, on request of an officer, appear for an examination."
30. Section 16 (2) states: "In the case of a foreign national,
    a. The relevant evidence referred to in subsection (1) includes photographic and fingerprint evidence; and
    b. Subject to the regulations, the foreign national must submit to a medical examination."
31. Section 18 (1) of *IRPA* states: "Subject to the regulations, every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

Immigration and Refugee Protection Act (IRPA) – examination authorities

32. Section 15 (1) of the *IRPA* states: "An officer is authorized to proceed with an examination if a person makes an application to the officer in accordance with this Act or if an application is made under subsection 11(1.01)."[3]
33. Section 15 (3) of the *IRPA* states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies of extracts and hold the means of transportation until the inspection and examination are completed."

[3] Section 11 (1.01) of the *IRPA* addresses mandatory electronic travel authorizations made by foreign nationals prior to entry.

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

34. Section 16 (3) of the *IRPA* states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."
35. Section 139 of the *IRPA* states: "An officer may search any person seeking to come into Canada and may search their luggage and personal effects and the means of transportation that conveyed the person to Canada if the officer believes on reasonable grounds that the person
    a. has not revealed their identity or has hidden on or about their person documents that are relevant to their admissibility; or
    b. has committed, or possess documents that may be used in the commission of, an offence referred to in section 117, 118, or 122."

***Immigration and Refugee Protection Act* – seizure authority**

36. Section 140 (1) of the *IRPA* states: "An officer may seize and hold any means of transportation, document or other thing if the officer believes on reasonable grounds that it was fraudulently or improperly obtained or used or that the seizure is necessary to prevent its fraudulent or improper use or to carry out the purposes of this Act."

Immigration and Refugee Protection Act – Copying Authorities

37. Section 15(3) of the IRPA states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies or extracts and hold the means of transportation until the inspection and examination are completed."

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

38. Section 16(3) of the IRPA states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."

Roles and Responsibilities

Role of Border Services Officers

39. BSOs working at ports of entry must be familiar with the policy on the examination of travellers' digital devices.
40. BSOs are responsible for taking the mandatory training on the Examination of Digital Devices
41. BSOs are responsible for adhering to this policy on the examination of travellers' digital devices.
42. As per the policy guidance contained herein, BSOs are responsible for:
    a. remaining sensitive to the potential private nature of data stored on digital devices;
    b. following guidance on when and how digital devices can be examined;
    c. reporting any examinations of travellers' digital devices to CBSA Headquarters; and
    d. making accurate, contemporaneous and detailed notes whenever a traveller's digital device is examined.

Role of Intelligence Officers

43. Intelligence Officers are responsible for:

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

a. Familiarizing themselves with the policy on examinations of travellers' digital devices, and
b. Remaining available to consult with other CBSA Officers who may examine travellers' digital devices, including BSOs that encounter lookouts when processing travellers, to provide additional information to the BSO that could assist the BSO in determining if a digital device examination is justified.

Role of Superintendents

44. Superintendents are responsible for:

a. Familiarizing themselves with the policy on examinations of travellers' digital devices;
b. Ensuring BSOs working in the traveller continuum familiarize themselves with the policy on examinations of travellers' digital devices; and
c. Ensuring BSOs follow the policy guidance contained herein, including but not limited to:
    i. Not conducting digital device exams as a matter of course;
    ii. Taking accurate, contemporaneous and detailed notes when devices are examined;
    iii. Remaining sensitive to the potential private nature of these goods; and
    iv. Reporting to CBSA HQ all instances of examinations of travellers' digital devices.
d. Performing periodic compliance verifications to ensure BSOs are following the policies contained herein.

Role of Chiefs

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

45. Chiefs are responsible for:
    a. Ensuring ports of entry in their jurisdiction are aware of the policy on examinations of travellers' digital devices;
    b. Ensuring BSOs in their jurisdiction have completed the requisite training on the examination of digital devices;
    c. Ensuring Superintendents exercise due diligence in reporting instances of digital device examinations to CBSA Headquarters; and
    d. Ensuring Superintendents perform periodic compliance verifications to ensure BSOs are following the policies contained herein, including note taking.

Policies and Procedures

When a Traveller's Digital Device Can Be Examined

46. Examinations of travellers' digital devices must be performed with a clear link to administering or enforcing CBSA program legislation that governs the cross-border movement of people and goods, including animals and plants.
47. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence under any Act of Parliament.
48. See the section on Encountering Evidence of a Criminal Nature in this policy for further instruction.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Notetaking

53. Accurate, contemporaneous and detailed record-keeping in officer notebooks is essential when conducting examinations of travellers' digital devices.
54. These note taking requirements must be followed even in the instance that the examination of a traveller's digital device is non-resultant.
55. The note taking directives described herein consider the Supreme Court of Canada jurisprudence in inland contexts in relation to the obligation to keep a careful record when conducting a search of a digital device in the absence either of judicial authorization or reasonable and probable grounds. The note taking directives aim to protect CBSA Officers and support CBSA's legal authorities. Courts have also recognized that the record-keeping requirement will have the incidental effect of helping Officers focus on the question of whether their conduct in relation to the examination of the device falls squarely within the parameters of a lawful examination for CBSA program legislation purposes.

56. Accurate, contemporaneous and detailed note taking will:
    a. Assist Officers in being able to articulate each step of a CBSA port of entry digital device examination for the purposes of CBSA program legislation;
    b. Serve as evidence should legal proceedings ensue;
    c. Protect the officer and the CBSA should allegations of misconduct arise through internal CBSA complaint mechanisms or external review or complaint bodies; and

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

d. Serve as a record of the judicious and lawful use of the statutory authorities available to officers.

57. The note taking directives contained herein are in addition to the note taking requirements identified in the agency's Notebook Policy, found in Part 8, Chapter 1 of the Enforcement Manual.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

59. Any information examined residing on a traveller's digital device must be linked to relevant legislated CBSA program concerns[5] and the examination must take place within the scope of an applicable lawful authority.

60. Section 16 (3) of the *IRPA* authorizes an Officer to require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence that may be used to establish their identity or compliance with the *IRPA*. Where an Officer has concerns regarding identity or non-compliance with the *IRPA*, they may examine relevant data on the permanent resident or foreign national's digital device, as reasonably required, to determine identity or non-compliance under the *IRPA*.

61. Sections 34 through 42 of the *IRPA* set out the conditions under which a foreign national or permanent resident is inadmissible to Canada. Where an Officer has concerns that an

[5] CBSA program legislation is defined in section 2 of the *Canada Border Service Agency Act*.

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

individual may be inadmissible, they may examine relevant data on the traveller's digital device, as reasonably required, to determine admissibility.

62. In terms of importation, under section 99 (1) (a) of the *Customs Act* only goods that have been imported are subject to examination by CBSA Officers, up until the time of release.
63. Therefore, CBSA Officers are only authorized by section 99 (1) (a) of the *Customs Act* to examine data that resides on a digital device at the time of importation, at any time up to the time of release.
64. To avoid mistakenly examining data not residing on the device at the time of importation, officers should take steps to disable network connectivity before the examination begins: See the Disabling Network Connectivity section below.

Privacy and Presence of Traveller

65. CBSA Officers must remain cognisant of the potential private nature of data stored on travellers' devices, remain sensitive, discreet and professional to minimize potential embarrassment to travellers.
66. Digital devices and media may hold data related to, for example, personal photos, journal entries, text messages, group chats, travel history, intimate imagery, medical information and medical history (see the Encountering intimate images and other sensitive material section), legal advice (see the Solicitor-Client privileged and Judicial information section), financial information, and other private details.
67. Where operationally feasible, Officers should perform examinations of travellers' digital devices in the presence of the traveller to mitigate against potential concerns of the traveller.
68. When a traveller is present for the examination, Officers should be prepared to explain:
    a. the authority under which they are conducting the examination;

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

b. the rationale(s) for the examination, if appropriate; and
c. that no information will be seized or any data copied unless required as evidence of a contravention or offence.

Device Passwords and Security

69. Digital devices are frequently protected with a password or other security method (e.g. passcode, biometrics, etc.). In order for an Officer to examine a digital device a traveller must supply the means for the device to be examined.
70. Where a password is required to gain access to a digital device, Officers should explain to a traveller that a password must be supplied in order for the traveller's obligations on entry to Canada under the *Customs* Act, the *IRPA* or other CBSA program legislation to be fulfilled.
71. While a device may primarily be protected by a biometrics-enabled method, the device can often also be accessed through a password. Where possible, Officers should seek to gain access to devices using this latter type of security method.

73. Officers should notate a device's password on a separate piece of paper in order to ensure it can be accessed at a later date, should prohibited content or evidence be found (see the Note taking directives section for more information).
74. If the examination is resultant, Officers should copy the password from the separate piece of paper into their officer notebook.
75. If the examination of a digital device is non-resultant, Officers should not retain the password or passcode. Officers should provide the traveller with the piece of paper upon

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

which they recorded the password or passcode. Officers should record that they have done so in their officer notebook.

76. Officers shall inform the traveller that their password or passcode, if retained, will be protected in accordance with privacy legislation.
77. After a non-resultant examination, Officers shall inform the traveller that their password or passcode can be changed immediately.
78. Officers should not record passwords to travellers' digital devices in CBSA systems, including the Integrated Customs Enforcement System (ICES) or the Integrated Customs System (ICS).

    Note: Officers should continue to use standard operating procedures to submit passwords to the Prohibited Importations Unit.

Disabling Network Connectivity

79. CBSA Officers must only access data that is stored on a traveller's digital device and must not access **any data** stored remotely.
80. In order to prevent accessing remote data, Officers should, before beginning the examination, deactivate its network connectivity.
81. Officers should note the if they were able to deactivate network connectivity in their notebooks.
82. Deactivating network connectivity can also prevent remote wiping or locking.
83. Activating "airplane mode" **may not disable all** network connectivity. Officers must ensure that the device is not connected to a WiFi network, wirelessly tethered to another device, or is sharing a connection with another device via Bluetooth.
84. Normally the status of network connectivity is indicated by icons in the top of the screen. If unsure, an Officer may choose to open the settings of the device and verify connectivity.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

85. Officers may also ask the traveller how to disable network connectivity, however, the traveller should not perform this function themselves.

How a Device Should be Examined

86. Enforcement Manual Part 4, Chapter 3 addresses how Officers should conduct personal baggage, goods and conveyance examinations. This policy on port of entry examinations of travellers' digital devices offers further precision in respect of examining travellers' digital goods but should be read in conjunction with that chapter of the manual.
87. Enforcement Manual Part 4, Chapter 3 stipulates that all examinations by Officers must be conducted in strict adherence to the CBSA's core values. Examinations must be proficient and discrete to the extent possible with respect to travellers and their goods, and all examinations must be conducted in a courteous and professional manner in accordance with the CBSA *Code of Conduct*.
88. Just as secondary examinations should be methodical, progressive and responsive as new indicators or information is discovered by or revealed to the Officer, so should any secondary examination of a traveller's digital device.
89. An examination of a traveller's digital device should be tailored to the purposes of the CBSA program legislation and should not be conducted as a matter of course.
90. In order to expedite the examination and if practical, an Officer may ask the traveller to point to the relevant area of the device for which the Officer has CBSA border screening and processing concerns. Focussing the examination will maximize efficiency for the Officer and minimize inconvenience to the traveller.
91. As a matter of policy, a port of entry digital device examination should be limited to:
    a. the examination of content for concerns related to CBSA program legislation; and

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

b. areas of the device and data directly related to indicators or concerns identified by the Officer during the interaction with the traveller.

92. Officers should be able to clearly articulate their reasoning for examining each type of data on the device, its link to indicators or concerns identified by the Officer, and the data's anticipated relevance to CBSA program legislation.
93. If, during the examination, additional indicators of concern are observed, the examination may expand and progress beyond the Officer's initial intent, provided diligent notes are taken regarding how and why the examination progresses.
94. Port of entry examinations should only be conducted manually and without the assistance of software/hardware.

Copying/Reproducing Data From a Traveller's Digital Device

95. Officers shall advise the traveller that their information will be protected by CBSA in accordance with applicable law including the *Privacy Act* and the *Customs Act*.
96. Officers shall not make copies of, duplicate or reproduce data examined on digital devices, including taking photographs or screenshots, unless such copying is authorized in the circumstances under CBSA program legislation and required for the specific and direct administration or enforcement of CBSA program legislation.
97. Officers shall not notate in their notebook or record in a CBSA system personal any information including contacts, phone numbers, names, dates of birth or other information from devices unless such notating or recording is authorized in the circumstances under CBSA program legislation, and required for the specific and direct administration or enforcement of CBSA program legislation.
98. Officers may rely on their regulatory copying authorities appropriate to the circumstances (*Customs Act* 115(1), IRPA 15(3) or 16(3)) if the legislative criteria in the relevant authority

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

are met, and, only if the copying is for the specific and direct regulatory administration or enforcement of CBSA program legislation. In these cases, travellers are to be informed that their information has been copied and that their information will be protected by the CBSA in accordance with applicable law including the *Privacy Act* and *Customs Act.*

99. Officers must use a CBSA-issued camera for any copying and must note the timestamp on the photograph in their notebook.

Reporting of Digital Device Examination

101. Effective November 2017, all examinations of travellers' digital devices must be reported to CBSA Headquarters as per Operational Bulletin 2017-61.

102. It is the policy of the CBSA to nationally track:

   a. the number of examinations of travellers' digital devices;

   b. the date of the examinations; and

   c. the port of entry at which the examinations took place.

103. CBSA Officers are expected to record in their notebooks all other information pertaining to digital device exams as per the Note taking directives section (e.g. the indicators that led to the digital device examination, the areas of the device accessed, etc.).

Encountering Intimate Images and Other Sensitive Material

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

104. A traveller may be particularly concerned if intimate images[6] of themselves or others are saved on the device.

105. If a traveller alerts an Officer to the presence of intimate images of themselves or others, the Officer should ask the traveller if there is a way to reasonably circumvent the viewing of those images.

[6] Intimate image is defined in s. 162.1 (2) of the *Criminal Code*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

119. If an Officer believes that the examination would compromise the solicitor-client privilege or judicial information, the Officer should:

    a. Notify and consult with their immediate supervisor with respect to the circumstances; and
    b. Determine with the supervisor if the device should be released, or
    c. Detain (*Customs* Act 101) or seize (IRPA 140(1)) the device without being examined, seal the device in a package marked with the assumption they are privileged, and set the device aside for review by a court or analogous independent review body for confirmation of privilege.

120. Officers can contact their region's Justice Liaison Officer for information on how to proceed with confirmation of privilege.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

125. In these circumstances, officers must also be cognisant that continuing the examination could potentially alter digital evidence (e.g. timestamps indicating when the file was last accessed).

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Detention and seizure of device

129. Part 5, Chapters 2 and 3 of the Enforcement Manual are the primary guidance documents for the seizure of evidence and goods from travellers.

Refusal to provide means of accessing a digital device

130. During a border examination upon entry to Canada, travellers have the legal obligation under the *Customs Act* to provide the means to access their goods, including digital devices, as well as the obligation to produce all relevant evidence that an Officer reasonably requires under the *IRPA*.

131. Every reasonable opportunity should be given to the traveller to fulfill their obligations at the port of entry under CBSA program legislation in providing the means to access their digital device.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

133. During the course of a regulatory examination of a traveller's digital device at secondary, assistance to gain access to the device shall not be obtained from any source outside the CBSA.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Sharing of information or data discovered on a traveller's digital device

139. The CBSA's primary guidance document on disclosure of "customs information," as defined in Section 107 of the ***Customs Act,*** is the Policy on the Disclosure of Customs Information: Section 107 of the *Customs Act*. This document should guide CBSA Officers when determining if they may provide access to customs information, in any form (e.g. hard copy, electronic or video format).

140. If information collected during a secondary examination does not meet the definition of "customs information" but instead meets the definition of "personal information" as defined in the *Privacy Act,* CBSA Officers should consult the Policy on the Disclosure of Personal Information: Section 8 of the *Privacy Act* for guidance.

Accompanying Resources

141. This policy document is not intended to be a standalone document, and should be read in conjunction with the following resources:

Canada Border Services Agency Act
Customs Act
Immigration and Refugee Protection Act
Privacy Act
Criminal Code
Canada Border Services Agency Code of Conduct
Canada Border Services Agency Enforcement Manual

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Enforcement Manual
Operational Bulletins
Shift Briefing Bulletins
Training and Learning products

Please note: This is not an exhaustive list of resources; the list will be updated as policy changes are made.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

ENFORCEMENT MANUAL

Part 4

EXAMINATION – GOODS AND CONVEYANCES

Chapter 16

POLICY ON PORT OF ENTRY EXAMINATIONS OF TRAVELLERS' DIGITAL DEVICES

June 2021

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

POLICY STATEMENT **3**

DEFINITIONS **3**

PURPOSE AND SCOPE **3**

AUTHORITIES – CUSTOMS ACT / IRPA **5**

ROLES AND RESPONSIBILITIES **11**

ROLE OF BORDER SERVICES OFFICERS 11
ROLE OF INTELLIGENCE OFFICERS 12
ROLE OF SUPERINTENDENTS 12
ROLE OF CHIEFS 13

POLICIES AND PROCEDURES **13**

WHEN A TRAVELLER'S DIGITAL DEVICE CAN BE EXAMINED 13
NOTE TAKING 15
WHAT CAN BE EXAMINED 17
PRIVACY AND PRESENCE OF TRAVELLER 18
DEVICE PASSWORDS AND SECURITY 19
DISABLING NETWORK CONNECTIVITY 20
HOW A DEVICE SHOULD BE EXAMINED 21
COPYING/REPRODUCING DATA FROM A TRAVELLER'S DIGITAL DEVICE 22
REPORTING OF DIGITAL DEVICE EXAMINATION 23
ENCOUNTERING INTIMATE IMAGES AND OTHER SENSITIVE MATERIAL 24
..... 25
SOLICITOR-CLIENT PRIVILEGED INFORMATION AND JUDICIAL INFORMATION 25
ENCOUNTERING EVIDENCE OF A CRIMINAL NATURE 27
DIGITAL DEVICE EXAMINATIONS AND LOOKOUT PROCEDURES 28

DETENTION AND SEIZURE OF DEVICE **28**

REFUSAL TO PROVIDE MEANS OF ACCESSING A DIGITAL DEVICE **28**

SHARING OF INFORMATION OR DATA DISCOVERED ON A TRAVELLER'S DIGITAL DEVICE **30**

ACCOMPANYING RESOURCES **31**

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Policy Statement

1. Digital devices, media, documents, software and stored electronic data are considered "goods" under Canada Border Services Agency (CBSA) program legislation and are subject to examination by CBSA Officers at ports of entry/customs offices (hereafter "ports of entry") for the administration and enforcement of CBSA program legislation. Examinations of digital devices and media can facilitate informed decision-making regarding admissibility and entry of people and goods to Canada under CBSA program legislation. CBSA Officers carrying out examinations of travellers' digital goods shall adhere to this policy.
2. Though digital devices are considered goods and can be examined as such, as a matter of policy, examinations of digital devices should not be conducted as a matter of course.

Definitions

3. "Digital device" for the purposes of this policy means mobile phones (cell phones), smartphones, computers, tablets, removable media, drives, cameras, smartwatches, and any other device capable of storing digital data in the actual possession or accompanying baggage of the traveller.
4. If a CBSA Officer is unsure as to whether a digital device is capable of storing digital data the Officer must include the device within the definition of digital device.
5. "CBSA program legislation" is defined in section 2 of the *Canada Border Services Agency Act*.

Purpose and Scope

6. The purpose of this policy is to provide CBSA Officers with a framework for the lawful, reasonable and progressive port of entry examinations of travellers' digital devices while

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

recognizing and respecting the potential private nature of information contained within these devices[1].

7. CBSA Officers, as with other non-digital information encountered, are bound to maintain the confidentiality of this information, except where sharing is permitted by law.
8. This policy applies to any CBSA Officer[2] who may, as part of their duties, examine a traveller's digital device as part of a secondary examination under the *Customs Act* or the *Immigration and Refugee Protection Act* (IRPA) at a port of entry.
9. This policy applies to inbound, port of entry examinations of travellers' digital devices.
10. This policy does not apply to commercial quantities of digital devices, or digital devices imported for commercial purposes.
11. This policy does not apply to examinations performed under section 99.3 of the *Customs Act* (see Enforcement Manual Part 6, Chapter 9 – Customs Controlled Areas).
12. This policy does not apply to instances where a traveller's digital device is examined or searched:
    a. to determine if physical (i.e. non-digital) contraband is contained within or on the device itself (ex: contraband hidden in a cavity within a device);
    b. under judicial authorization (i.e. search warrant);
    c. incident to arrest;
    d. in relation to *IRPA* A16(1) or A16(3), when applied outside of the port of entry context (e.g. overseas or within Canada);
    e. solely to determine if the digital device functions; or

[1] In a criminal investigative inland context, Canadian courts have recognized that digital devices can have unique characteristics that differentiate them from other items subject to a search

[2] The CBSA employee must meet the definition of "officer" under the relevant provisions of the *Customs Act* and the *IRPA* to conduct these examinations under both the *Customs Act* and the *IRPA*

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

f. when a traveller displays digital content to an Officer, in an attempt to demonstrate compliance with CBSA program legislation or to provide additional context or information relevant to their admissibility or compliance (ex: a digital copy of a work or study permit, or receipts to show the value of an item), provided the viewing of that content by the Officer does not progress to a more detailed examination of the device's contents not initially displayed to the Officer.

Note: When the above 11. f) circumstances are met, CBSA Officers must still ensure that any subsequent obtaining of information from the interaction is within the scope of lawful authority and is for valid CBSA program legislation purposes.

13. This policy does not limit any examination authority conferred on any CBSA Officer under any Act of Parliament.

Authorities – Customs Act / IRPA

14. The *Customs Act* and IRPA authorities to examine digital devices by CBSA Officers at the border can remain available throughout an interaction with a traveller until the examination or assessment is completed. Possible concerns such as identity, admissibility of persons, smuggling and/or release of goods can occur simultaneously.

    Note: CBSA Officers must be mindful of distinctions as between CBSA's relevant authorities (eg.: IRPA 16(3) does not apply to Canadian citizens whereas IRPA 139 requires reasonable grounds to believe)."

15. If a digital device examination is performed simultaneously for non-compliance under both the *Customs Act* and the *IRPA,* the examining Officer must adhere simultaneously to the specific legislative criteria under the specific legislative examination authorities on which the

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Officer is relying to conduct the digital device examination at the port of entry, as well as this policy.

16. If a digital device examination progresses to require further exercise of CBSA authorities (eg.: obtaining, detaining, seizing, etc.), the relevant officer must continue to adhere to the specific legislative authority's requirements and associated CBSA policy guidance appropriate to the circumstances.

Customs Act – Obligations of Travellers

17. Section 7.1 of the *Customs Act* states: "Any information provided to an officer in the administration or enforcement of this Act, the *Customs Tariff* or the *Special Import Measures Act* or under any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, shall be true, accurate and complete."
18. Section 11 (1) of the *Customs Act* states: "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present [themselves]to an officer and answer truthfully any questions asked by the officer in the performance of [their] duties under this or any other Act of Parliament."
19. Section 12 (1) of the *Customs Act* states: "all goods that are imported shall, except in such circumstances and subject to such conditions as may be prescribed, be reported at the nearest customs office designated for that purpose that is open for business."
20. Section 13 of the *Customs Act* states: "Every person who reports goods under section 12 inside or outside Canada or is stopped by an officer in accordance with section 99.1 shall

    (a) answer truthfully any question asked by an officer with respect to the goods; and

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

(b) if an officer so requests, present the goods to the officer, remove any covering from the goods, unload any conveyance or open any part of the conveyance, or open or unpack any package or container that the officer wishes to examine."

***Customs Act* - Examination of Goods Authorities**

21. Section 99 (1) (a) of the *Customs Act* allows an officer: "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;"
22. Section 99 (1) (e) of the *Customs Act* states: "where the officer suspects on reasonable grounds that this Act or the regulations or any other Act of Parliament administered or enforced by [them] or any regulations thereunder have been or might be contravened in respect of any goods, examine the goods and open or cause to be opened any package or container thereof;"

***Customs Act* – Detention of Goods Authority**

23. Section 101 of the *Customs Act* states: "goods that have been imported or are about to be exported may be detained by an officer until [they are] satisfied that the goods have been dealt with in accordance with this Act, and any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, and any regulations made thereunder."

***Customs Act* – Seizure of Goods Authority**

24. Section 110 (1) (a) of the *Customs Act* states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened in respect of goods, seize as forfeit

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

a. The goods;"

25. Section 110 (3) states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened, seize anything that [they believe] on reasonable grounds will afford evidence in respect of the contravention."

Customs Act – Copying Authority

26. Section 115(1) states: "If any record is examined or seized under this Act, the Minister, or the officer by whom it is examined or seized, may make or cause to be made one or more copies of it, and a copy purporting to be certified by the Minister or a person authorized by the Minister is admissible in evidence and has the same probative force as the original would have if it had been proved in the ordinary way."

***Criminal Code* – Seizure without warrant**

27. Section 489 (2) of the Criminal Code states: "Every peace officer, and every public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, who is lawfully present in a place pursuant to a warrant or otherwise in the execution of duties, may, without a warrant, seize any thing that the officer believes on reasonable grounds

    a. has been obtained by the commission of an offence against this or any other Act of Parliament;
    b. has been used in the commission of an offence against this or any other Act of Parliament; or
    c. will afford evidence in respect of an offence against this or any other Act of Parliament.

Immigration and Refugee Protection Act (IRPA) – obligations of persons seeking entry

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

28. Section 16 (1) of the *IRPA* states: "A person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires."
29. Section 16 (1.1) states: "A person who makes an application must, on request of an officer, appear for an examination."
30. Section 16 (2) states: "In the case of a foreign national,
    a. The relevant evidence referred to in subsection (1) includes photographic and fingerprint evidence; and
    b. Subject to the regulations, the foreign national must submit to a medical examination."
31. Section 18 (1) of *IRPA* states: "Subject to the regulations, every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

Immigration and Refugee Protection Act (IRPA) – examination authorities

32. Section 15 (1) of the *IRPA* states: "An officer is authorized to proceed with an examination if a person makes an application to the officer in accordance with this Act or if an application is made under subsection 11(1.01)."[3]
33. Section 15 (3) of the *IRPA* states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies of extracts and hold the means of transportation until the inspection and examination are completed."

[3] Section 11 (1.01) of the *IRPA* addresses mandatory electronic travel authorizations made by foreign nationals prior to entry.

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

34. Section 16 (3) of the *IRPA* states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."
35. Section 139 of the *IRPA* states: "An officer may search any person seeking to come into Canada and may search their luggage and personal effects and the means of transportation that conveyed the person to Canada if the officer believes on reasonable grounds that the person
    a. has not revealed their identity or has hidden on or about their person documents that are relevant to their admissibility; or
    b. has committed, or possess documents that may be used in the commission of, an offence referred to in section 117, 118, or 122."

***Immigration and Refugee Protection Act* – seizure authority**

36. Section 140 (1) of the *IRPA* states: "An officer may seize and hold any means of transportation, document or other thing if the officer believes on reasonable grounds that it was fraudulently or improperly obtained or used or that the seizure is necessary to prevent its fraudulent or improper use or to carry out the purposes of this Act."

Immigration and Refugee Protection Act – Copying Authorities

37. Section 15(3) of the IRPA states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies or extracts and hold the means of transportation until the inspection and examination are completed."

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

38. Section 16(3) of the IRPA states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."

Roles and Responsibilities

Role of Border Services Officers

39. BSOs working at ports of entry must be familiar with the policy on the examination of travellers' digital devices.
40. BSOs are responsible for taking the mandatory training on the Examination of Digital Devices (S7188-P)
41. BSOs are responsible for adhering to this policy on the examination of travellers' digital devices.
42. As per the policy guidance contained herein, BSOs are responsible for:
    a. requesting supervisor approval before conducting a digital device examination;
    b. remaining sensitive to the potential private nature of data stored on digital devices;
    c. following guidance on when and how digital devices can be examined;
    d. reporting any examinations of travellers' digital devices to CBSA Headquarters;
    e. making accurate, contemporaneous and detailed notes whenever a traveller's digital device is examined;
    f. submitting the notes to the supervisor for review; and
    g. completing the notes appropriately if the supervisor determines they are not sufficient.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Role of Intelligence Officers

43. Intelligence Officers are responsible for:

    a. Familiarizing themselves with the policy on examinations of travellers' digital devices, and

    b. Remaining available to consult with other CBSA Officers who may examine travellers' digital devices, including BSOs that encounter lookouts when processing travellers, to provide additional information to the BSO that could assist the BSO in determining if a digital device examination is justified.

Role of Superintendents

44. Superintendents are responsible for:

    a. Familiarizing themselves with the policy on examinations of travellers' digital devices;

    b. Ensuring BSOs working in the traveller continuum familiarize themselves with the policy on examinations of travellers' digital devices;

    c. Ensuring BSOs follow the policy guidance contained herein, including but not limited to:

        i. Not conducting digital device exams as a matter of course;

        ii. Taking accurate, contemporaneous and detailed notes when devices are examined;

        iii. Remaining sensitive to the potential private nature of these goods; and

        iv. Reporting to CBSA HQ all instances of examinations of travellers' digital devices.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

d. Performing periodic compliance verifications to ensure BSOs are following the policies contained herein;
e. Approving and reviewing digital device exams performed by BSOs; and
f. Ensure the completion of the Examination of Digital Device (S7188-P) online training by all BSOs.

Role of Chiefs

45. Chiefs are responsible for:

a. Ensuring ports of entry in their jurisdiction are aware of the policy on examinations of travellers' digital devices;
b. Ensuring BSOs in their jurisdiction have completed the requisite training on the examination of digital devices;
c. Ensuring Superintendents exercise due diligence in reporting instances of digital device examinations to CBSA Headquarters; and
d. Ensuring Superintendents perform periodic compliance verifications to ensure BSOs are following the policies contained herein, including notetaking.
e. Approving and reviewing digital device exams performed by BSOs; and
f. Ensure the completion of the Examination of Digital Device (S7188-P) online training by all BSOs.

Policies and Procedures

When a Traveller's Digital Device Can Be Examined

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

46. Examinations of travellers' digital devices must be performed with a clear link to administering or enforcing CBSA program legislation that governs the cross-border movement of people and goods, including animals and plants.
47. CBSA officers are only permitted to perform a digital device examination if they have completed the Examination of Digital Devices training (S7188-P).
48. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence under any Act of Parliament.
49. See the section on Encountering Evidence of a Criminal Nature in this policy for further instruction.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Notetaking

54. Accurate, contemporaneous and detailed record-keeping in officer notebooks is essential when conducting examinations of travellers' digital devices.
55. These notetaking requirements must be followed even in the instance that the examination of a traveller's digital device is non-resultant.
56. The note taking directives described herein consider the Supreme Court of Canada jurisprudence in inland contexts in relation to the obligation to keep a careful record when conducting a search of a digital device in the absence either of judicial authorization or reasonable and probable grounds. The note taking directives aim to protect CBSA Officers and support CBSA's legal authorities. Courts have also recognized that the record-keeping requirement will have the incidental effect of helping Officers focus on the question of whether their conduct in relation to the examination of the device falls squarely within the parameters of a lawful examination for CBSA program legislation purposes.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

57. Accurate, contemporaneous and detailed note taking will:

    a. Assist Officers in being able to articulate each step of a CBSA port of entry digital device examination for the purposes of CBSA program legislation;

    b. Serve as evidence should legal proceedings ensue;

    c. Protect the officer and the CBSA should allegations of misconduct arise through internal CBSA complaint mechanisms or external review or complaint bodies; and

    d. Serve as a record of the judicious and lawful use of the statutory authorities available to officers.

58. The note taking directives contained herein are in addition to the note taking requirements identified in the agency's Notebook Policy, found in Part 8, Chapter 1 of the Enforcement Manual.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

60. Any information examined residing on a traveller's digital device must be linked to relevant legislated CBSA program concerns[5] and the examination must take place within the scope of an applicable lawful authority.

[5] CBSA program legislation is defined in section 2 of the *Canada Border Service Agency Act*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

61. Section 16 (3) of the *IRPA* authorizes an Officer to require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence that may be used to establish their identity or compliance with the *IRPA*. Where an Officer has concerns regarding identity or non-compliance with the *IRPA*, they may examine relevant data on the permanent resident or foreign national's digital device, as reasonably required, to determine identity or non-compliance under the *IRPA*.
62. Sections 34 through 42 of the *IRPA* set out the conditions under which a foreign national or permanent resident is inadmissible to Canada. Where an Officer has concerns that an individual may be inadmissible, they may examine relevant data on the traveller's digital device, as reasonably required, to determine admissibility.
63. In terms of importation, under section 99 (1) (a) of the *Customs Act* only goods that have been imported are subject to examination by CBSA Officers, up until the time of release.
64. Therefore, CBSA Officers are only authorized by section 99 (1) (a) of the *Customs Act* to examine data that resides on a digital device at the time of importation, at any time up to the time of release.
65. To avoid mistakenly examining data not residing on the device at the time of importation, officers should take steps to disable network connectivity before the examination begins: See the Disabling Network Connectivity section below.

Privacy and Presence of Traveller

66. CBSA Officers must remain cognisant of the potential private nature of data stored on travellers' devices, remain sensitive, discreet and professional to minimize potential embarrassment to travellers.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

67. Digital devices and media may hold data related to, for example, personal photos, journal entries, text messages, group chats, travel history, intimate imagery, medical information and medical history (see the Encountering intimate images and other sensitive material section), legal advice (see the Solicitor-Client privileged and Judicial information section), financial information, and other private details.
68. Where operationally feasible, Officers should perform examinations of travellers' digital devices in the presence of the traveller to mitigate against potential concerns of the traveller.
69. When a traveller is present for the examination, Officers should be prepared to explain:
    a. the authority under which they are conducting the examination;
    b. the rationale(s) for the examination, if appropriate; and
    c. that no information will be seized or any data copied unless required as evidence of a contravention or offence.

Device Passwords and Security

70. Digital devices are frequently protected with a password or other security method (e.g. passcode, biometrics, etc.). In order for an Officer to examine a digital device a traveller must supply the means for the device to be examined.
71. Where a password is required to gain access to a digital device, Officers should explain to a traveller that a password must be supplied in order for the traveller's obligations on entry to Canada under the *Customs* Act, the *IRPA* or other CBSA program legislation to be fulfilled.
72. While a device may primarily be protected by a biometrics-enabled method, the device can often also be accessed through a password. Where possible, Officers should seek to gain access to devices using this latter type of security method.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

74. Officers should notate a device's password on a separate piece of paper in order to ensure it can be accessed at a later date, should prohibited content or evidence be found (see the Note taking directives section for more information).
75. If the examination is resultant, Officers should copy the password from the separate piece of paper into their officer notebook.
76. If the examination of a digital device is non-resultant, Officers should not retain the password or passcode. Officers should provide the traveller with the piece of paper upon which they recorded the password or passcode. Officers should record that they have done so in their officer notebook.
77. Officers shall inform the traveller that their password or passcode, if retained, will be protected in accordance with privacy legislation.
78. After a non-resultant examination, Officers shall inform the traveller that their password or passcode can be changed immediately.
79. Officers should not record passwords to travellers' digital devices in CBSA systems, including the Integrated Customs Enforcement System (ICES) or the Integrated Customs System (ICS).

    Note: Officers should continue to use standard operating procedures to submit passwords to the Prohibited Importations Unit.

Disabling Network Connectivity

80. CBSA Officers must only access data that is stored on a traveller's digital device and must not access **any data** stored remotely.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

81. In order to prevent accessing remote data, Officers should, before beginning the examination, deactivate its network connectivity.
82. Officers should note the if they were able to deactivate network connectivity in their notebooks.
83. Deactivating network connectivity can also prevent remote wiping or locking.
84. Activating "airplane mode" **may not disable all** network connectivity. Officers must ensure that the device is not connected to a WiFi network, wirelessly tethered to another device, or is sharing a connection with another device via Bluetooth.
85. Normally the status of network connectivity is indicated by icons in the top of the screen. If unsure, an Officer may choose to open the settings of the device and verify connectivity.
86. Officers may also ask the traveller how to disable network connectivity, however, the traveller should not perform this function themselves.

How a Device Should be Examined

87. Enforcement Manual Part 4, Chapter 3 addresses how Officers should conduct personal baggage, goods and conveyance examinations. This policy on port of entry examinations of travellers' digital devices offers further precision in respect of examining travellers' digital goods but should be read in conjunction with that chapter of the manual.
88. Enforcement Manual Part 4, Chapter 3 stipulates that all examinations by Officers must be conducted in strict adherence to the CBSA's core values. Examinations must be proficient and discrete to the extent possible with respect to travellers and their goods, and all examinations must be conducted in a courteous and professional manner in accordance with the CBSA *Code of Conduct*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

89. Just as secondary examinations should be methodical, progressive and responsive as new indicators or information is discovered by or revealed to the Officer, so should any secondary examination of a traveller's digital device.
90. An examination of a traveller's digital device should be tailored to the purposes of the CBSA program legislation and should not be conducted as a matter of course.
91. In order to expedite the examination and if practical, an Officer may ask the traveller to point to the relevant area of the device for which the Officer has CBSA border screening and processing concerns. Focussing the examination will maximize efficiency for the Officer and minimize inconvenience to the traveller.
92. As a matter of policy, a port of entry digital device examination should be limited to:
    a. the examination of content for concerns related to CBSA program legislation; and
    b. areas of the device and data directly related to indicators or concerns identified by the Officer during the interaction with the traveller.
93. Officers should be able to clearly articulate their reasoning for examining each type of data on the device, its link to indicators or concerns identified by the Officer, and the data's anticipated relevance to CBSA program legislation.
94. If, during the examination, additional indicators of concern are observed, the examination may expand and progress beyond the Officer's initial intent, provided diligent notes are taken regarding how and why the examination progresses.
95. Port of entry examinations should only be conducted manually and without the assistance of software/hardware.

Copying/Reproducing Data From a Traveller's Digital Device

96. Officers shall advise the traveller that their information will be protected by CBSA in accordance with applicable law including the *Privacy Act* and the *Customs Act*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

97. Officers shall not make copies of, duplicate or reproduce data examined on digital devices, including taking photographs or screenshots, unless such copying is authorized in the circumstances under CBSA program legislation and required for the specific and direct administration or enforcement of CBSA program legislation.
98. Officers shall not notate in their notebook or record in a CBSA system personal any information including contacts, phone numbers, names, dates of birth or other information from devices unless such notating or recording is authorized in the circumstances under CBSA program legislation, and required for the specific and direct administration or enforcement of CBSA program legislation.
99. Officers may rely on their regulatory copying authorities appropriate to the circumstances (*Customs Act* 115(1), IRPA 15(3) or 16(3)) if the legislative criteria in the relevant authority are met, and, only if the copying is for the specific and direct regulatory administration or enforcement of CBSA program legislation. In these cases, travellers are to be informed that their information has been copied and that their information will be protected by the CBSA in accordance with applicable law including the *Privacy Act* and *Customs Act*.
100. Officers must use a CBSA-issued camera for any copying and must note the timestamp on the photograph in their notebook.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

102. Effective November 2017, all examinations of travellers' digital devices must be reported to CBSA Headquarters as per Operational Bulletin 2017-61.

103. It is the policy of the CBSA to nationally track:

a. the number of examinations of travellers' digital devices;

b. the date of the examinations; and

c. the port of entry at which the examinations took place.

104. CBSA Officers are expected to record in their notebooks all other information pertaining to digital device exams as per the Note taking directives section (e.g. the indicators that led to the digital device examination, the areas of the device accessed, etc.).

Encountering Intimate Images and Other Sensitive Material

105. A traveller may be particularly concerned if intimate images[6] of themselves or others are saved on the device.

106. If a traveller alerts an Officer to the presence of intimate images of themselves or others, the Officer should ask the traveller if there is a way to reasonably circumvent the viewing of those images.

[6] Intimate image is defined in s. 162.1 (2) of the *Criminal Code*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

120. If an Officer believes that the examination would compromise the solicitor-client privilege or judicial information, the Officer should:

    a. Notify and consult with their immediate supervisor with respect to the circumstances; and
    b. Determine with the supervisor if the device should be released, or
    c. Detain (*Customs* Act 101) or seize (IRPA 140(1)) the device without being examined, seal the device in a package marked with the assumption they are

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

privileged, and set the device aside for review by a court or analogous independent review body for confirmation of privilege.

121. Officers can contact their region's Justice Liaison Officer for information on how to proceed with confirmation of privilege.

Encountering Evidence of a Criminal Nature

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

126. In these circumstances, officers must also be cognisant that continuing the examination could potentially alter digital evidence (e.g. timestamps indicating when the file was last accessed).

Digital Device Examinations and Lookout Procedures

Detention and seizure of device

130. Part 5, Chapters 2 and 3 of the Enforcement Manual are the primary guidance documents for the seizure of evidence and goods from travellers.

Refusal to provide means of accessing a digital device

131. During a border examination upon entry to Canada, travellers have the legal obligation under the *Customs Act* to provide the means to access their goods, including digital devices, as well as the obligation to produce all relevant evidence that an Officer reasonably requires under the *IRPA*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

132. Every reasonable opportunity should be given to the traveller to fulfill their obligations at the port of entry under CBSA program legislation in providing the means to access their digital device.

134. During the course of a regulatory examination of a traveller's digital device at secondary, assistance to gain access to the device shall not be obtained from any source outside the CBSA.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Sharing of information or data discovered on a traveller's digital device

140. The CBSA's primary guidance document on disclosure of "customs information," as defined in Section 107 of the *Customs Act,* is the Policy on the Disclosure of Customs Information: Section 107 of the *Customs Act*. This document should guide CBSA Officers when determining if they may provide access to customs information, in any form (e.g. hard copy, electronic or video format).

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information.

141. If information collected during a secondary examination does not meet the definition of "customs information" but instead meets the definition of "personal information" as defined in the *Privacy Act,* CBSA Officers should consult the Policy on the Disclosure of Personal Information: Section 8 of the *Privacy Act* for guidance.

Accompanying Resources

142. This policy document is not intended to be a standalone document, and should be read in conjunction with the following resources:

Canada Border Services Agency Act
Customs Act
Immigration and Refugee Protection Act
Privacy Act
Criminal Code
Canada Border Services Agency Code of Conduct
Canada Border Services Agency Enforcement Manual
Enforcement Manual
Operational Bulletins
Shift Briefing Bulletins
Training and Learning products

Please note: This is not an exhaustive list of resources; the list will be updated as policy changes are made.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

ENFORCEMENT MANUAL

Part 4

EXAMINATION – GOODS AND CONVEYANCES

Chapter 16

POLICY ON PORT OF ENTRY EXAMINATIONS OF TRAVELLERS' DIGITAL DEVICES

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

POLICY STATEMENT **3**

DEFINITIONS **3**

PURPOSE AND SCOPE **3**

AUTHORITIES – CUSTOMS ACT / IRPA **5**

ROLES AND RESPONSIBILITIES **11**

ROLE OF BORDER SERVICES OFFICERS 11
ROLE OF INTELLIGENCE OFFICERS 12
ROLE OF SUPERINTENDENTS 12
ROLE OF CHIEFS 13

POLICIES AND PROCEDURES **13**

WHEN A TRAVELLER'S DIGITAL DEVICE CAN BE EXAMINED 14
NOTE TAKING 15
WHAT CAN BE EXAMINED 17
PRIVACY AND PRESENCE OF TRAVELLER 19
DEVICE PASSWORDS AND SECURITY 19
DISABLING NETWORK CONNECTIVITY 21
HOW A DEVICE SHOULD BE EXAMINED 21
COPYING/REPRODUCING DATA FROM A TRAVELLER'S DIGITAL DEVICE 23
REPORTING OF DIGITAL DEVICE EXAMINATION 24
ENCOUNTERING INTIMATE IMAGES AND OTHER SENSITIVE MATERIAL 24
..... 25
SOLICITOR-CLIENT PRIVILEGED INFORMATION AND JUDICIAL INFORMATION 25
ENCOUNTERING EVIDENCE OF A CRIMINAL NATURE 27
DIGITAL DEVICE EXAMINATIONS AND LOOKOUT PROCEDURES 28

DETENTION AND SEIZURE OF DEVICE **28**

REFUSAL TO PROVIDE MEANS OF ACCESSING A DIGITAL DEVICE **29**

SHARING OF INFORMATION OR DATA DISCOVERED ON A TRAVELLER'S DIGITAL DEVICE **30**

ACCOMPANYING RESOURCES **31**

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Policy Statement

1. Digital devices, media, documents, software and stored electronic data are considered "goods" under Canada Border Services Agency (CBSA) program legislation and are subject to examination by CBSA Officers at ports of entry/customs offices (hereafter "ports of entry") for the administration and enforcement of CBSA program legislation. Examinations of digital devices and media can facilitate informed decision-making regarding admissibility and entry of people and goods to Canada under CBSA program legislation. CBSA Officers carrying out examinations of travellers' digital goods shall adhere to this policy.
2. Though digital devices are considered goods and can be examined as such, as a matter of policy, examinations of digital devices should not be conducted as a matter of course.

Definitions

3. "Digital device" for the purposes of this policy means mobile phones (cell phones), smartphones, computers, tablets, removable media, drives, cameras, smartwatches, and any other device capable of storing digital data in the actual possession or accompanying baggage of the traveller.
4. If a CBSA Officer is unsure as to whether a digital device is capable of storing digital data the Officer must include the device within the definition of digital device.
5. "CBSA program legislation" is defined in section 2 of the *Canada Border Services Agency Act*.

Purpose and Scope

6. The purpose of this policy is to provide CBSA Officers with a framework for the lawful, reasonable and progressive port of entry examinations of travellers' digital devices while

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

recognizing and respecting the potential private nature of information contained within these devices[1].

Note: The Agency has an overarching policy regarding notetaking. Please refer to the CBSA Enforcement Manual Part 8, Chapter 1 – Notebooks and Notetaking by Officers at Ports of Entry for guidance on the proper use of the Officer Notebook (BSF556) and the application of sound notetaking principles.

7. CBSA Officers, as with other non-digital information encountered, are bound to maintain the confidentiality of this information, except where sharing is permitted by law.
8. This policy applies to any CBSA Officer[2] who may, as part of their duties, examine a traveller's digital device as part of a secondary examination under the *Customs Act* or the *Immigration and Refugee Protection Act* (IRPA) at a port of entry.
9. This policy applies to inbound, port of entry examinations of travellers' digital devices.
10. This policy does not apply to commercial quantities of digital devices, or digital devices imported for commercial purposes.
11. This policy does not apply to examinations performed under section 99.3 of the *Customs Act* (see Enforcement Manual Part 6, Chapter 9 – Customs Controlled Areas).
12. This policy does not apply to instances where a traveller's digital device is examined or searched:
    a. to determine if physical (i.e. non-digital) contraband is contained within or on the device itself (ex: contraband hidden in a cavity within a device);
    b. under judicial authorization (i.e. search warrant);
    c. incident to arrest;

[1] In a criminal investigative inland context, Canadian courts have recognized that digital devices can have unique characteristics that differentiate them from other items subject to a search

[2] The CBSA employee must meet the definition of "officer" under the relevant provisions of the *Customs Act* and the *IRPA* to conduct these examinations under both the *Customs Act* and the *IRPA*

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

d. in relation to *IRPA* A16(1) or A16(3), when applied outside of the port of entry context (e.g. overseas or within Canada);
e. solely to determine if the digital device functions; or
f. when a traveller displays digital content to an Officer, in an attempt to demonstrate compliance with CBSA program legislation or to provide additional context or information relevant to their admissibility or compliance (ex: a digital copy of a work or study permit, or receipts to show the value of an item), provided the viewing of that content by the Officer does not progress to a more detailed examination of the device's contents not initially displayed to the Officer.

Note: When the above 11. f) circumstances are met, CBSA Officers must still ensure that any subsequent obtaining of information from the interaction is within the scope of lawful authority and is for valid CBSA program legislation purposes.

13. This policy does not limit any examination authority conferred on any CBSA Officer under any Act of Parliament.

Authorities – Customs Act / IRPA

14. The *Customs Act* and IRPA authorities to examine digital devices by CBSA Officers at the border can remain available throughout an interaction with a traveller until the examination or assessment is completed. Possible concerns such as identity, admissibility of persons, smuggling and/or release of goods can occur simultaneously.

    Note: CBSA Officers must be mindful of distinctions as between CBSA's relevant authorities (eg.: IRPA 16(3) does not apply to Canadian citizens whereas IRPA 139 requires reasonable grounds to believe)."

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

15. If a digital device examination is performed simultaneously for non-compliance under both the *Customs Act* and the *IRPA,* the examining Officer must adhere simultaneously to the specific legislative criteria under the specific legislative examination authorities on which the Officer is relying to conduct the digital device examination at the port of entry, as well as this policy.
16. If a digital device examination progresses to require further exercise of CBSA authorities (eg.: obtaining, detaining, seizing, etc.), the relevant officer must continue to adhere to the specific legislative authority's requirements and associated CBSA policy guidance appropriate to the circumstances.

Customs Act – Obligations of Travellers

17. Section 7.1 of the *Customs Act* states: "Any information provided to an officer in the administration or enforcement of this Act, the *Customs Tariff* or the *Special Import Measures Act* or under any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, shall be true, accurate and complete."
18. Section 11 (1) of the *Customs Act* states: "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present [themselves]to an officer and answer truthfully any questions asked by the officer in the performance of [their] duties under this or any other Act of Parliament."
19. Section 12 (1) of the *Customs Act* states: "all goods that are imported shall, except in such circumstances and subject to such conditions as may be prescribed, be reported at the nearest customs office designated for that purpose that is open for business."
20. Section 13 of the *Customs Act* states: "Every person who reports goods under section 12 inside or outside Canada or is stopped by an officer in accordance with section 99.1 shall

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

(a) answer truthfully any question asked by an officer with respect to the goods; and

(b) if an officer so requests, present the goods to the officer, remove any covering from the goods, unload any conveyance or open any part of the conveyance, or open or unpack any package or container that the officer wishes to examine."

***Customs Act* - Examination of Goods Authorities**

21. Section 99 (1) (a) of the *Customs Act* allows an officer: "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;"

22. Section 99 (1) (e) of the *Customs Act* states: "where the officer suspects on reasonable grounds that this Act or the regulations or any other Act of Parliament administered or enforced by [them] or any regulations thereunder have been or might be contravened in respect of any goods, examine the goods and open or cause to be opened any package or container thereof;"

***Customs Act* – Detention of Goods Authority**

23. Section 101 of the *Customs Act* states: "goods that have been imported or are about to be exported may be detained by an officer until [they are] satisfied that the goods have been dealt with in accordance with this Act, and any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, and any regulations made thereunder."

***Customs Act* – Seizure of Goods Authority**

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

24. Section 110 (1) (a) of the *Customs Act* states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened in respect of goods, seize as forfeit

    a. The goods;"

25. Section 110 (3) states: "An officer may, where [they believe] on reasonable grounds that this Act or the regulations have been contravened, seize anything that [they believe] on reasonable grounds will afford evidence in respect of the contravention."

***Customs Act* – Copying Authority**

26. Section 115(1) states: "If any record is examined or seized under this Act, the Minister, or the officer by whom it is examined or seized, may make or cause to be made one or more copies of it, and a copy purporting to be certified by the Minister or a person authorized by the Minister is admissible in evidence and has the same probative force as the original would have if it had been proved in the ordinary way."

***Criminal Code* – Seizure without warrant**

27. Section 489 (2) of the Criminal Code states: "Every peace officer, and every public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, who is lawfully present in a place pursuant to a warrant or otherwise in the execution of duties, may, without a warrant, seize any thing that the officer believes on reasonable grounds

    a. has been obtained by the commission of an offence against this or any other Act of Parliament;

    b. has been used in the commission of an offence against this or any other Act of Parliament; or

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

c. will afford evidence in respect of an offence against this or any other Act of Parliament.

Immigration and Refugee Protection Act (IRPA) – obligations of persons seeking entry

28. Section 16 (1) of the *IRPA* states: "A person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires."
29. Section 16 (1.1) states: "A person who makes an application must, on request of an officer, appear for an examination."
30. Section 16 (2) states: "In the case of a foreign national,
    a. The relevant evidence referred to in subsection (1) includes photographic and fingerprint evidence; and
    b. Subject to the regulations, the foreign national must submit to a medical examination."
31. Section 18 (1) of *IRPA* states: "Subject to the regulations, every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

Immigration and Refugee Protection Act (IRPA) – examination authorities

32. Section 15 (1) of the *IRPA* states: "An officer is authorized to proceed with an examination if a person makes an application to the officer in accordance with this Act or if an application is made under subsection 11(1.01)."[3]

[3] Section 11 (1.01) of the *IRPA* addresses mandatory electronic travel authorizations made by foreign nationals prior to entry.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

33. Section 15 (3) of the *IRPA* states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies of extracts and hold the means of transportation until the inspection and examination are completed."
34. Section 16 (3) of the *IRPA* states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."
35. Section 139 of the *IRPA* states: "An officer may search any person seeking to come into Canada and may search their luggage and personal effects and the means of transportation that conveyed the person to Canada if the officer believes on reasonable grounds that the person
    a. has not revealed their identity or has hidden on or about their person documents that are relevant to their admissibility; or
    b. has committed, or possess documents that may be used in the commission of, an offence referred to in section 117, 118, or 122."

***Immigration and Refugee Protection Act* – seizure authority**

36. Section 140 (1) of the *IRPA* states: "An officer may seize and hold any means of transportation, document or other thing if the officer believes on reasonable grounds that it was fraudulently or improperly obtained or used or that the seizure is necessary to prevent its fraudulent or improper use or to carry out the purposes of this Act."

Immigration and Refugee Protection Act – Copying Authorities

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

37. Section 15(3) of the IRPA states: "An officer may board and inspect any means of transportation bringing persons to Canada, examine any person carried by that means of transportation and any record or document respecting that person, seize and remove the record or document to obtain copies or extracts and hold the means of transportation until the inspection and examination are completed."
38. Section 16(3) of the IRPA states: "An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."

Roles and Responsibilities

Role of Border Services Officers

39. BSOs working at ports of entry must be familiar with the policy on the examination of travellers' digital devices.
40. BSOs are responsible for taking the mandatory training on the Examination of Digital Devices (S7188-P)
41. BSOs are responsible for adhering to this policy on the examination of travellers' digital devices.
42. As per the policy guidance contained herein, BSOs are responsible for:
    a. requesting supervisor approval before conducting a digital device examination;
    b. remaining sensitive to the potential private nature of data stored on digital devices;
    c. following guidance on when and how digital devices can be examined;
    d. reporting any examinations of travellers' digital devices to CBSA Headquarters;

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

e. making accurate, contemporaneous and detailed notes whenever a traveller's digital device is examined;
f. submitting the notes to the supervisor for review; and
g. completing the notes appropriately if the supervisor determines they are not sufficient.

Role of Intelligence Officers

43. Intelligence Officers are responsible for:

a. Familiarizing themselves with the policy on examinations of travellers' digital devices, and
b. Remaining available to consult with other CBSA Officers who may examine travellers' digital devices, including BSOs that encounter lookouts when processing travellers, to provide additional information to the BSO that could assist the BSO in determining if a digital device examination is justified.

Role of Superintendents

44. Superintendents are responsible for:

a. Familiarizing themselves with the policy on examinations of travellers' digital devices;
b. Ensuring BSOs working in the traveller continuum familiarize themselves with the policy on examinations of travellers' digital devices;
c. Ensuring BSOs follow the policy guidance contained herein, including but not limited to:
    i. Not conducting digital device exams as a matter of course;

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

ii. Taking accurate, contemporaneous and detailed notes when devices are examined;

iii. Remaining sensitive to the potential private nature of these goods; and

iv. Reporting to CBSA HQ all instances of examinations of travellers' digital devices.

d. Performing periodic compliance verifications to ensure BSOs are following the policies contained herein;

e. Approving and reviewing digital device exams performed by BSOs; and

f. Ensure the completion of the Examination of Digital Device (S7188-P) online training by all BSOs.

Role of Chiefs

45. Chiefs are responsible for:

a. Ensuring ports of entry in their jurisdiction are aware of the policy on examinations of travellers' digital devices;

b. Ensuring BSOs in their jurisdiction have completed the requisite training on the examination of digital devices;

c. Ensuring Superintendents exercise due diligence in reporting instances of digital device examinations to CBSA Headquarters; and

d. Ensuring Superintendents perform periodic compliance verifications to ensure BSOs are following the policies contained herein, including notetaking.

e. Approving and reviewing digital device exams performed by BSOs; and

f. Ensure the completion of the Examination of Digital Device (S7188-P) online training by all BSOs.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

When a Traveller's Digital Device Can Be Examined

46. Examinations of travellers' digital devices must be performed with a clear link to administering or enforcing CBSA program legislation that governs the cross-border movement of people and goods, including animals and plants.
47. CBSA officers are only permitted to perform a digital device examination if they have completed the Examination of Digital Devices training (S7188-P).
48. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence under any Act of Parliament.
49. See the section on Encountering Evidence of a Criminal Nature in this policy for further instruction.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Notetaking

54. Accurate, contemporaneous and detailed record-keeping in officer notebooks is essential when conducting examinations of travellers' digital devices.
55. These notetaking requirements must be followed even in the instance that the examination of a traveller's digital device is non-resultant.
56. The note taking directives described herein consider the Supreme Court of Canada jurisprudence in inland contexts in relation to the obligation to keep a careful record when conducting a search of a digital device in the absence either of judicial authorization or reasonable and probable grounds. The note taking directives aim to protect CBSA Officers and support CBSA's legal authorities. Courts have also recognized that the record-keeping

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

requirement will have the incidental effect of helping Officers focus on the question of whether their conduct in relation to the examination of the device falls squarely within the parameters of a lawful examination for CBSA program legislation purposes.

57. Accurate, contemporaneous and detailed note taking will:
    a. Assist Officers in being able to articulate each step of a CBSA port of entry digital device examination for the purposes of CBSA program legislation;
    b. Serve as evidence should legal proceedings ensue;
    c. Protect the officer and the CBSA should allegations of misconduct arise through internal CBSA complaint mechanisms or external review or complaint bodies; and
    d. Serve as a record of the judicious and lawful use of the statutory authorities available to officers.
58. The note taking directives contained herein are in addition to the note taking requirements identified in the agency's Notebook Policy, found in Part 8, Chapter 1 of the Enforcement Manual.

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

60. Any information examined residing on a traveller's digital device must be linked to relevant legislated CBSA program concerns[5] and the examination must take place within the scope of an applicable lawful authority.
61. Section 16 (3) of the *IRPA* authorizes an Officer to require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence that may be used to establish their identity or compliance with the *IRPA*. Where an Officer has concerns regarding identity or non-compliance with the *IRPA*, they may examine relevant data on the permanent resident or foreign national's digital device, as reasonably required, to determine identity or non-compliance under the *IRPA*.
62. Sections 34 through 42 of the *IRPA* set out the conditions under which a foreign national or permanent resident is inadmissible to Canada. Where an Officer has concerns that an individual may be inadmissible, they may examine relevant data on the traveller's digital device, as reasonably required, to determine admissibility.
63. In terms of importation, under section 99 (1) (a) of the *Customs Act* only goods that have been imported are subject to examination by CBSA Officers, up until the time of release.
64. Therefore, CBSA Officers are only authorized by section 99 (1) (a) of the *Customs Act* to examine data that resides on a digital device at the time of importation, at any time up to the time of release.
65. To avoid mistakenly examining data not residing on the device at the time of importation, officers should take steps to disable network connectivity before the examination begins: See the Disabling Network Connectivity section below.

[5] CBSA program legislation is defined in section 2 of the *Canada Border Service Agency Act*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Privacy and Presence of Traveller

66. CBSA Officers must remain cognisant of the potential private nature of data stored on travellers' devices, remain sensitive, discreet and professional to minimize potential embarrassment to travellers.
67. Digital devices and media may hold data related to, for example, personal photos, journal entries, text messages, group chats, travel history, intimate imagery, medical information and medical history (see the Encountering intimate images and other sensitive material section), legal advice (see the Solicitor-Client privileged and Judicial information section), financial information, and other private details.
68. Where operationally feasible, Officers should perform examinations of travellers' digital devices in the presence of the traveller to mitigate against potential concerns of the traveller.
69. When a traveller is present for the examination, Officers should be prepared to explain:
    a. the authority under which they are conducting the examination;
    b. the rationale(s) for the examination, if appropriate; and
    c. that no information will be seized or any data copied unless required as evidence of a contravention or offence.

Device Passwords and Security

70. Digital devices are frequently protected with a password or other security method (e.g. passcode, biometrics, etc.). In order for an Officer to examine a digital device a traveller must supply the means for the device to be examined.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

71. Where a password is required to gain access to a digital device, Officers should explain to a traveller that a password must be supplied in order for the traveller's obligations on entry to Canada under the *Customs* Act, the *IRPA* or other CBSA program legislation to be fulfilled.
72. While a device may primarily be protected by a biometrics-enabled method, the device can often also be accessed through a password. Where possible, Officers should seek to gain access to devices using this latter type of security method.

74. Officers should notate a device's password on a separate piece of paper in order to ensure it can be accessed at a later date, should prohibited content or evidence be found (see the Note taking directives section for more information).
75. If the examination is resultant, Officers should copy the password from the separate piece of paper into their officer notebook.
76. If the examination of a digital device is non-resultant, Officers should not retain the password or passcode. Officers should provide the traveller with the piece of paper upon which they recorded the password or passcode. Officers should record that they have done so in their officer notebook.
77. Officers shall inform the traveller that their password or passcode, if retained, will be protected in accordance with privacy legislation.
78. After a non-resultant examination, Officers shall inform the traveller that their password or passcode can be changed immediately.
79. Officers should not record passwords to travellers' digital devices in CBSA systems, including the Integrated Customs Enforcement System (ICES) or the Integrated Customs System (ICS).

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Note: Officers should continue to use standard operating procedures to submit passwords to the Prohibited Importations Unit.

Disabling Network Connectivity

80. CBSA Officers must only access data that is stored on a traveller's digital device and must not access **any data** stored remotely.
81. In order to prevent accessing remote data, Officers should, before beginning the examination, deactivate its network connectivity.
82. Officers should note the if they were able to deactivate network connectivity in their notebooks.
83. Deactivating network connectivity can also prevent remote wiping or locking.
84. Activating "airplane mode" **may not disable all** network connectivity. Officers must ensure that the device is not connected to a WiFi network, wirelessly tethered to another device, or is sharing a connection with another device via Bluetooth.
85. Normally the status of network connectivity is indicated by icons in the top of the screen. If unsure, an Officer may choose to open the settings of the device and verify connectivity.
86. Officers may also ask the traveller how to disable network connectivity, however, the traveller should not perform this function themselves.

How a Device Should be Examined

87. Enforcement Manual Part 4, Chapter 3 addresses how Officers should conduct personal baggage, goods and conveyance examinations. This policy on port of entry examinations of travellers' digital devices offers further precision in respect of examining travellers' digital goods but should be read in conjunction with that chapter of the manual.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information.

88. Enforcement Manual Part 4, Chapter 3 stipulates that all examinations by Officers must be conducted in strict adherence to the CBSA's core values. Examinations must be proficient and discrete to the extent possible with respect to travellers and their goods, and all examinations must be conducted in a courteous and professional manner in accordance with the CBSA *Code of Conduct*.
89. Just as secondary examinations should be methodical, progressive and responsive as new indicators or information is discovered by or revealed to the Officer, so should any secondary examination of a traveller's digital device.
90. An examination of a traveller's digital device should be tailored to the purposes of the CBSA program legislation and should not be conducted as a matter of course.
91. In order to expedite the examination and if practical, an Officer may ask the traveller to point to the relevant area of the device for which the Officer has CBSA border screening and processing concerns. Focussing the examination will maximize efficiency for the Officer and minimize inconvenience to the traveller.
92. As a matter of policy, a port of entry digital device examination should be limited to:
    a. the examination of content for concerns related to CBSA program legislation; and
    b. areas of the device and data directly related to indicators or concerns identified by the Officer during the interaction with the traveller.
93. Officers should be able to clearly articulate their reasoning for examining each type of data on the device, its link to indicators or concerns identified by the Officer, and the data's anticipated relevance to CBSA program legislation.
94. If, during the examination, additional indicators of concern are observed, the examination may expand and progress beyond the Officer's initial intent, provided diligent notes are taken regarding how and why the examination progresses.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

95. Port of entry examinations should only be conducted manually and without the assistance of software/hardware.

Copying/Reproducing Data From a Traveller's Digital Device

96. Officers shall advise the traveller that their information will be protected by CBSA in accordance with applicable law including the *Privacy Act* and the *Customs Act*.
97. Officers shall not make copies of, duplicate or reproduce data examined on digital devices, including taking photographs or screenshots, unless such copying is authorized in the circumstances under CBSA program legislation and required for the specific and direct administration or enforcement of CBSA program legislation.
98. Officers shall not notate in their notebook or record in a CBSA system personal any information including contacts, phone numbers, names, dates of birth or other information from devices unless such notating or recording is authorized in the circumstances under CBSA program legislation, and required for the specific and direct administration or enforcement of CBSA program legislation.
99. Officers may rely on their regulatory copying authorities appropriate to the circumstances (*Customs Act* 115(1), IRPA 15(3) or 16(3)) if the legislative criteria in the relevant authority are met, and, only if the copying is for the specific and direct regulatory administration or enforcement of CBSA program legislation. In these cases, travellers are to be informed that their information has been copied and that their information will be protected by the CBSA in accordance with applicable law including the *Privacy Act* and *Customs Act.*
100. Officers must use a CBSA-issued camera for any copying and must note the timestamp on the photograph in their notebook.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Reporting of Digital Device Examination

102. Effective November 2017, all examinations of travellers' digital devices must be reported to CBSA Headquarters as per Operational Bulletin 2017-61.

103. It is the policy of the CBSA to nationally track:

a. the number of examinations of travellers' digital devices;

b. the date of the examinations; and

c. the port of entry at which the examinations took place.

104. CBSA Officers are expected to record in their notebooks all other information pertaining to digital device exams as per the Note taking directives section (e.g. the indicators that led to the digital device examination, the areas of the device accessed, etc.).

Encountering Intimate Images and Other Sensitive Material

105. A traveller may be particularly concerned if intimate images[6] of themselves or others are saved on the device.

106. If a traveller alerts an Officer to the presence of intimate images of themselves or others, the Officer should ask the traveller if there is a way to reasonably circumvent the viewing of those images.

[6] Intimate image is defined in s. 162.1 (2) of the *Criminal Code*.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

120. If an Officer believes that the examination would compromise the solicitor-client privilege or judicial information, the Officer should:

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

a. Notify and consult with their immediate supervisor with respect to the circumstances; and
b. Determine with the supervisor if the device should be released, or
c. Detain (*Customs* Act 101) or seize (IRPA 140(1)) the device without being examined, seal the device in a package marked with the assumption they are privileged, and set the device aside for review by a court or analogous independent review body for confirmation of privilege.

121. Officers can contact their region's Justice Liaison Officer for information on how to proceed with confirmation of privilege.

Encountering Evidence of a Criminal Nature

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

126. In these circumstances, officers must also be cognisant that continuing the examination could potentially alter digital evidence (e.g. timestamps indicating when the file was last accessed).

Digital Device Examinations and Lookout Procedures

Detention and seizure of device

130. Part 5, Chapters 2 and 3 of the Enforcement Manual are the primary guidance documents for the seizure of evidence and goods from travellers.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Refusal to provide means of accessing a digital device

131. During a border examination upon entry to Canada, travellers have the legal obligation under the *Customs Act* to provide the means to access their goods, including digital devices, as well as the obligation to produce all relevant evidence that an Officer reasonably requires under the *IRPA*.

132. Every reasonable opportunity should be given to the traveller to fulfill their obligations at the port of entry under CBSA program legislation in providing the means to access their digital device.

134. During the course of a regulatory examination of a traveller's digital device at secondary, assistance to gain access to the device shall not be obtained from any source outside the CBSA.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Sharing of information or data discovered on a traveller's digital device

140. The CBSA's primary guidance document on disclosure of "customs information," as defined in Section 107 of the *Customs Act,* is the Policy on the Disclosure of Customs

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Information: Section 107 of the *Customs Act*. This document should guide CBSA Officers when determining if they may provide access to customs information, in any form (e.g. hard copy, electronic or video format).

141. If information collected during a secondary examination does not meet the definition of "customs information" but instead meets the definition of "personal information" as defined in the *Privacy Act,* CBSA Officers should consult the Policy on the Disclosure of Personal Information: Section 8 of the *Privacy Act* for guidance.

Accompanying Resources

142. This policy document is not intended to be a standalone document, and should be read in conjunction with the following resources:

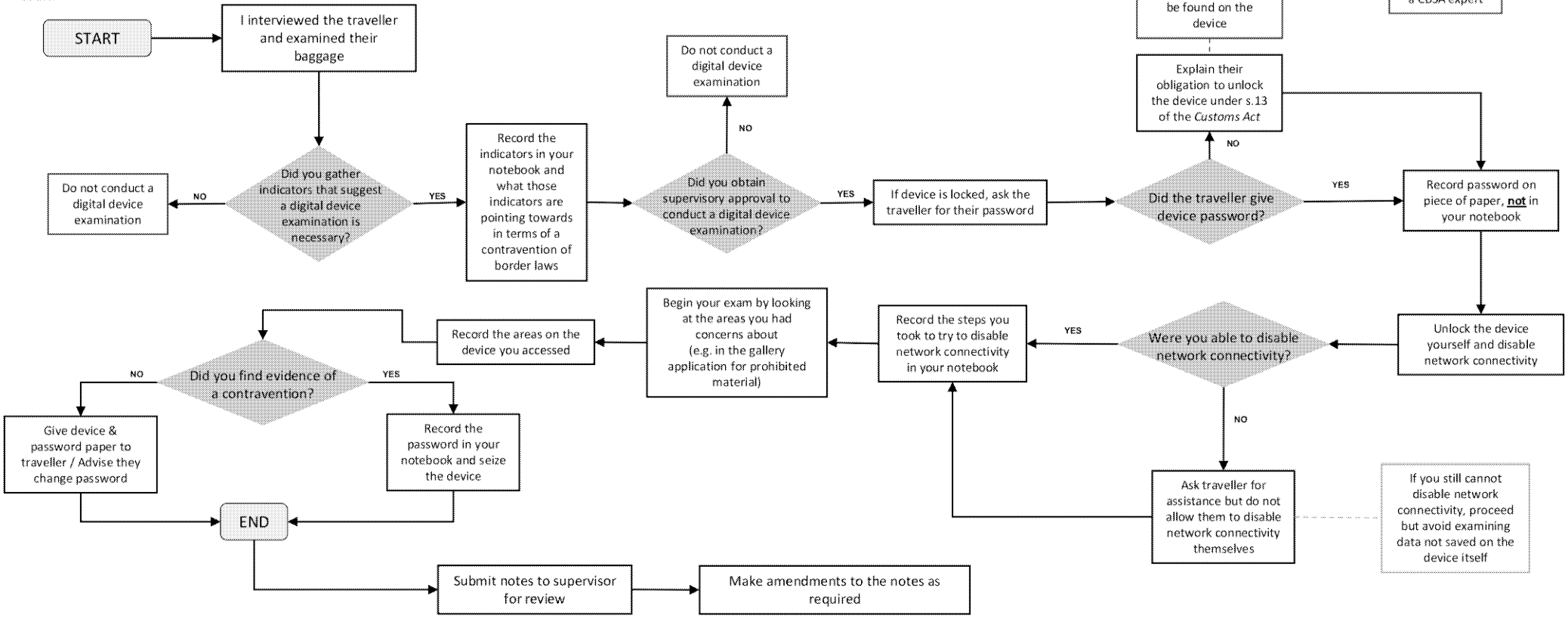
Canada Border Services Agency Act
Customs Act
Immigration and Refugee Protection Act
Privacy Act
Criminal Code
Canada Border Services Agency Code of Conduct
Canada Border Services Agency Enforcement Manual
Enforcement Manual
Operational Bulletins
Shift Briefing Bulletins
Training and Learning products

Please note: This is not an exhaustive list of resources; the list will be updated as policy changes are made.

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Conducting a digital device examination

The CBSA recognizes that digital devices can contain personal information, so it has placed a higher threshold for examining these devices among other goods. Due to the potential personal nature of device contents, travellers may be upset that their device is being examined. It is important that Officers are diligent in following the procedures for the examination of digital devices to prevent privacy complaints and to ensure the Agency's actions are defensible in court.



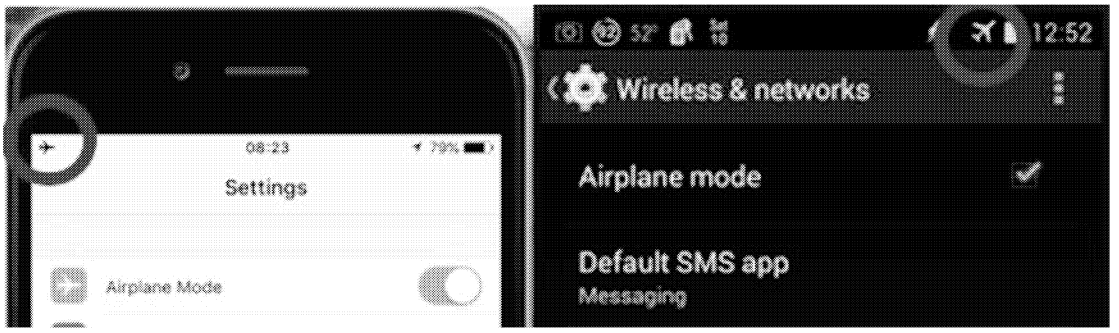
CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Cellphone Examination Technical Guide
Disabling Network Connectivity on Androids and iPhones

Steps to disable network connectivity must be taken before your examination can begin. This is to prevent access to information not stored directly on the device which cannot be examined and to prevent any potential remote wiping software from erasing potentially prohibited material. Generally, this can be accomplished by enabling 'airplane mode' on the device.

NOTE: A passenger may have their phone in airplane mode already from their flight. Verify this by looking at the top of the screen (on both androids and iphones) for the airplane symbol.

IPHONE **ANDROID**



If the passenger has not put their phone on airplane mode, below are some tips to help you do so:

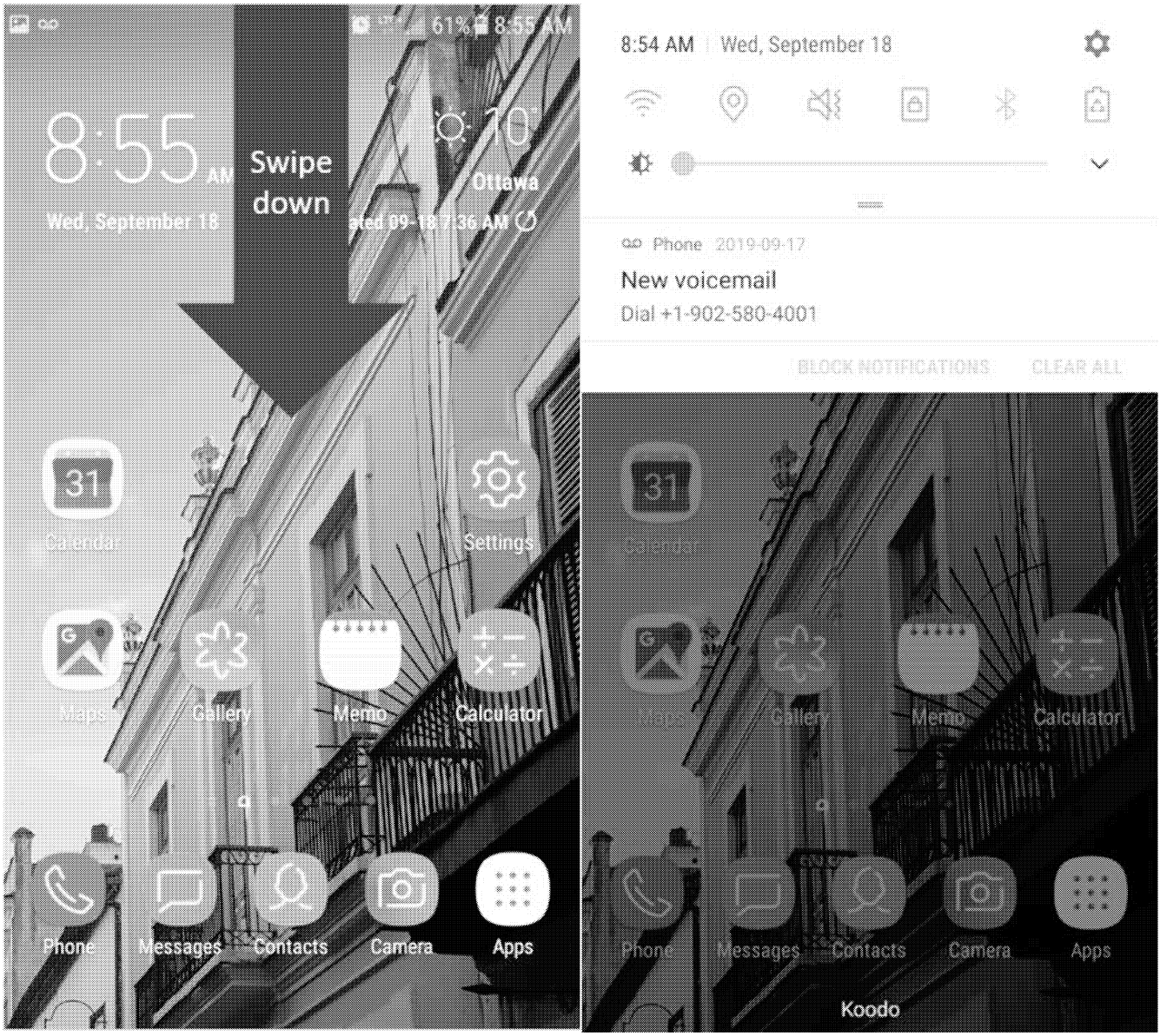
a) Android Phones

- **There are many models of Android phones, but most have a similar look and feel to their user interface. The following two methods of disabling connectivity should assist you with the majority of android devices.**

1. Method 1

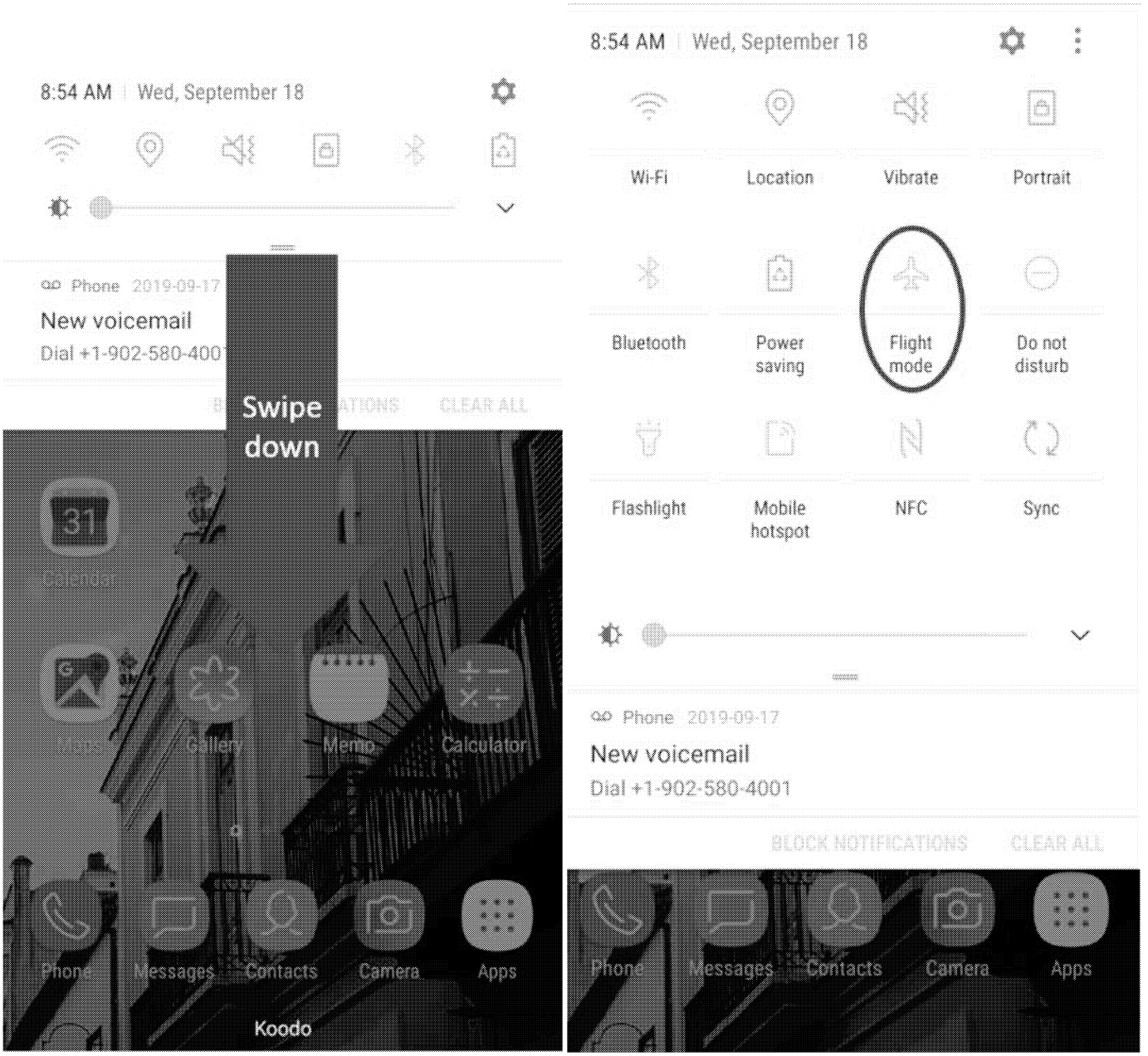
   i. Unlock device
   ii. Swipe down from the top of the screen

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information.



iii. If you cannot see the airplane symbol swipe down again

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information



iv. Tap flight mode
v. Verify the phone is in airplane/flight mode by looking for the airplane symbol at the top of the screen

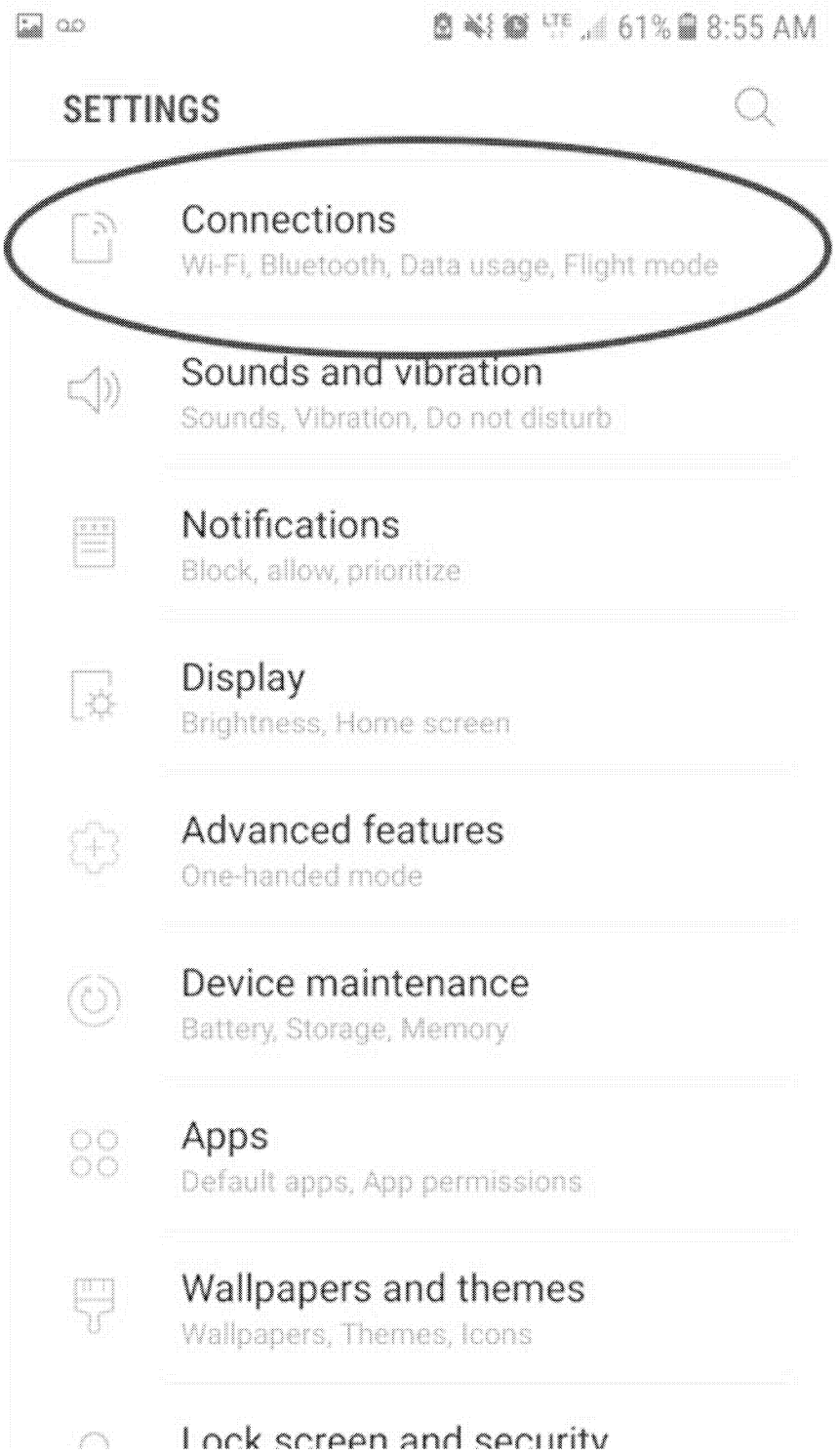
2. <u>Method 2</u>
   i. Unlock the device
   ii. Locate the settings application

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information



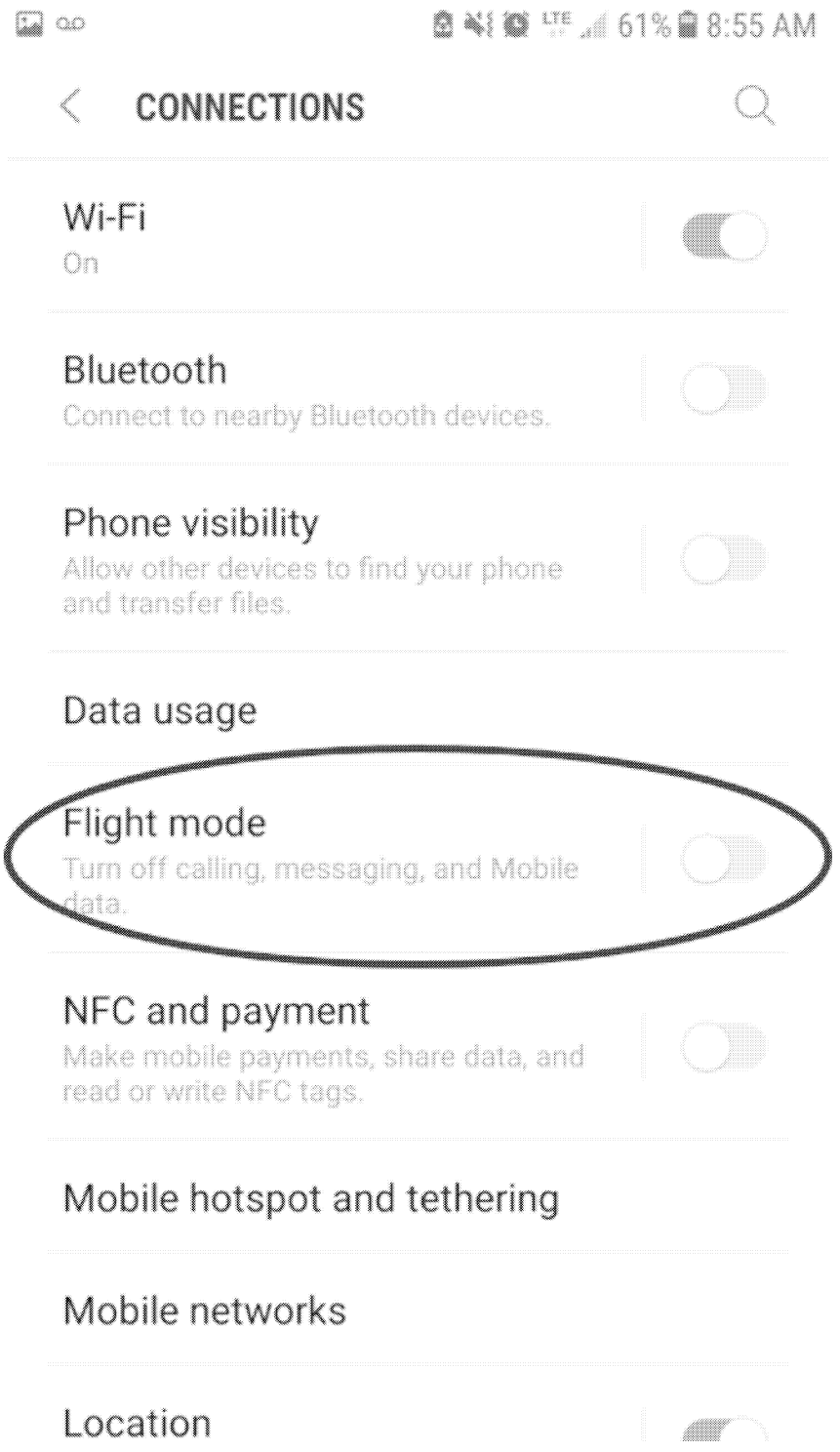
iii. If flight mode is not available on the first screen, tap connections (may also be called network)

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information



iv. You should then be able to enable flight mode

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information



v. Verify the phone is in airplane/flight mode by looking for the airplane symbol at the top of the screen

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

b) iPhones

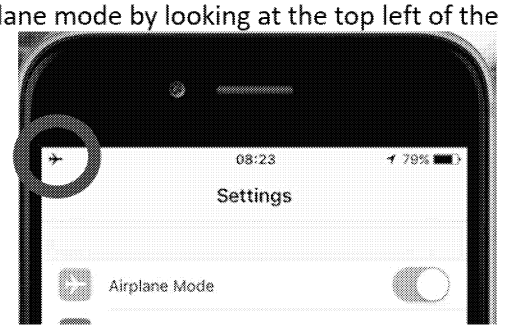
- **. Below are two methods to place any iPhone into airplane mode.**

1) Method 1

i. Unlock the device.
ii. Swipe up from the very bottom of the phone to open a control panel that looks like the second picture below.
iii. Tap the airplane symbol (second picture below in yellow)



iv. Verify that the phone is in airplane mode by looking at the top left of the screen for the airplane symbol.



CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

2) <u>Second method for enabling airplane mode on an iphone:</u>

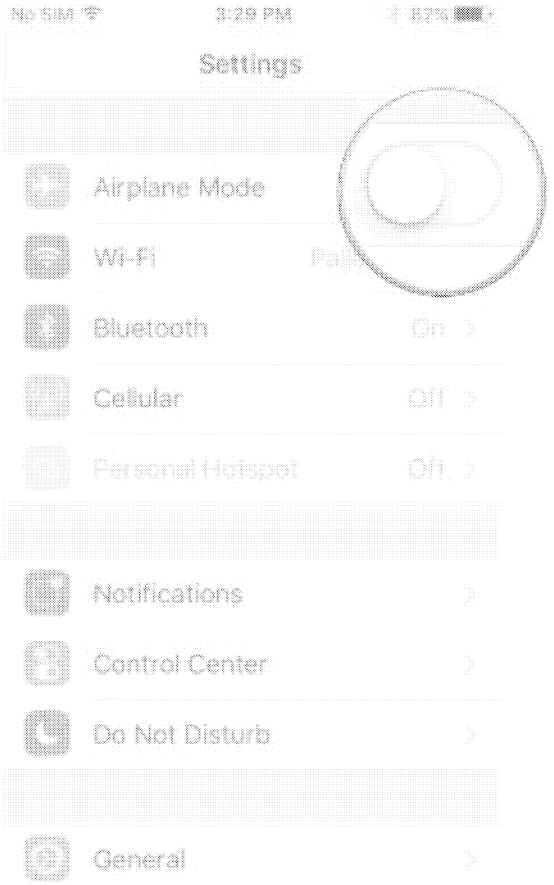
i. Unlock the device.

ii. Locate the settings icon on the phone. It may not be on the first screen, if you cannot find it swipe left to see more icons.

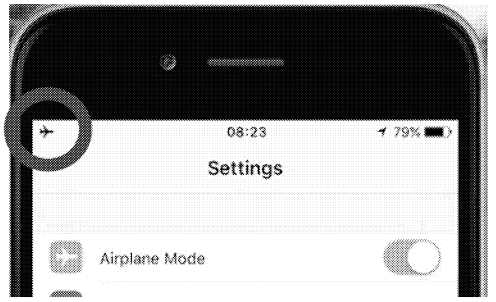


iii. Once you have the settings application open airplane mode will be at the top. Tap the switch to turn it on.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information



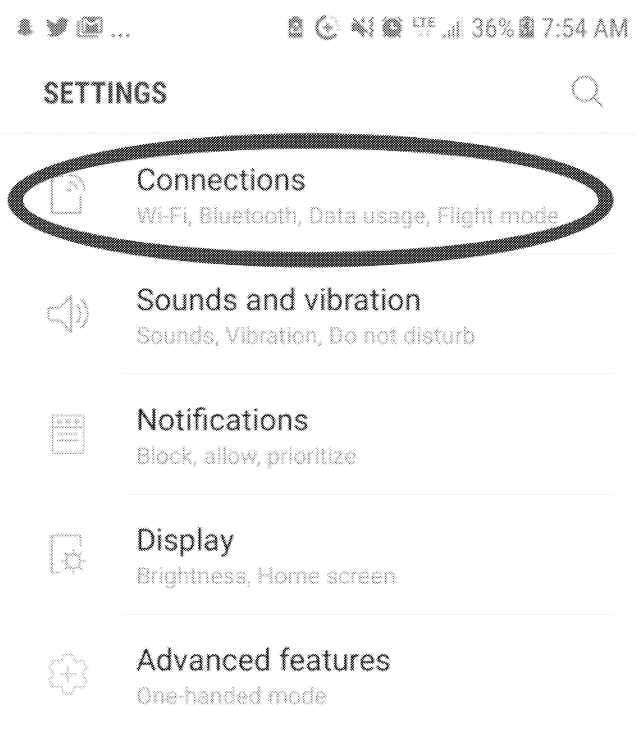
iv. Verify that the phone is in airplane mode by looking at the top of the screen for the airplane symbol.

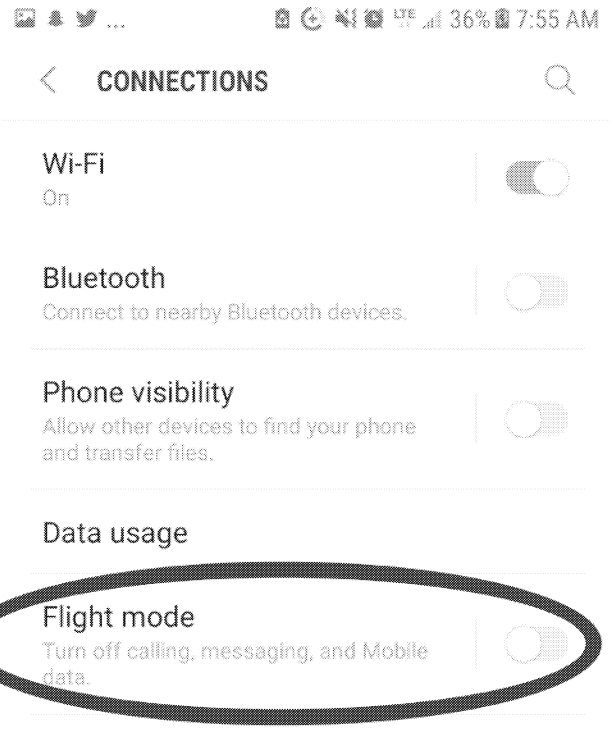


Other phones

If you cannot access airplane mode from swiping on the home screen, it will always be found in the settings of the phone. Sometimes you may need to tap a category such as 'network' or 'connections' to open up the option to turn on airplane mode, also sometimes called 'flight mode'.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information





CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

DIGITAL DEVICE EXAMINATIONS

NOTETAKING REQUIREMENTS: RATIONALE

The purpose of this job aid is to explain why each notetaking element is required in order to support a digital device examination.

Notetaking Requirement	Rationale
a) Local date and time, including the start and end time of the digital device examination	The CBSA has been reprimanded for spending an "unreasonable" amount of time examining a traveller's digital device. Recording the amount of time your examination actually took place will assist in refuting these claims.
b) Indicators observed by the officer	It is important to provide the indicators your observed in order to meet the requirement of having a multiplicity of indicators before beginning a digital device examination.
c) CBSA program legislation rationale for the examination (i.e. what are the indicators pointing towards? IRPA concerns, prohibited material, etc.)	Courts and the Office of the Privacy Commissioner have expressed concerns that examinations of digital devices are branching beyond IRPA and Customs Act concerns, particularly that these exams are moving into the realm of criminal investigations. Recording the Customs Act or IRPA-related rationale will support the purpose of your examination.
d) Type of device (e.g. Cellphone, laptop, etc.) and, if necessary to distinguish it from other devices of the same type, description of that device (e.g. Pink cellphone, Toshiba laptop, etc,)	This is simply to help officers recall what device they examined.
e) Only if examination is resultant, password(s) and any relevant security protection details (the password should be noted on a separate paper until it is determined the examination was resultant)	Though the CBSA has the authority to collect passwords as part of its examination of digital devices, there are elevated privacy concerns when it comes to retaining passwords unnecessarily (i.e. you have not seized the phone and do not require access later).
f) Steps taken to disable network connectivity	Only goods being imported into Canada are subject to examination. Therefore, only content resident on the device itself is subject to examination. Anything accessible through a network or stored on the cloud is not deemed to be imported.
g) Areas examined on the device (e.g. gallery, documents, gmail, etc.)	This will help refute claims that officers have opened applications not relevant to their concerns.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

h) Documents of interest (e.g. note a description of a photo suspected of being child pornography or note the name of a document with suspected evidence of IRPA misrepresentation)	It is important to note any evidence of contraventions that is uncovered.
i) If the rationale for your examination changes as new indicators arise (e.g. was for IRPA purposes but indicators of prohibited material have arisen) note that change in rationale	This is will help officers articulate what authorities they are using in the examination and will substantiate the legality of these examinations.
j) If relevant, the traveller's demeanor and any communication with respect to the device and its contents	Relevant details include any indicators that develop during the examination.
k) If assistance was obtained, note the individuals involved	It is important to account for anyone that was involved in an examination so all the relevant notes can be recovered and to provide proof that only those who required access to the device accessed it.
l) If any facilitative technology was used by CBSA experts (e.g. DFU provided unlocking services), note that	There are heightened sensitivities around the use of facilitative technology. It is important that the CBSA is transparent about the use of this technology and accounts for any support given to aid in the examination of digital devices.
m) If examination is resultant, note the next steps taken	It is important to include whether the device was seized or detained or any other details flowing from a resultant digital device examination.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

FULL LIST:

a) **Local date and time**, including the start and end time of the digital device examination;
b) **Indicators** observed by the officer;
c) CBSA **program legislation rationale** for the examination (i.e. what are the indicators pointing towards? IPRA concerns, prohibited material, etc.);
d) **Type of device** (e.g. Cellphone, laptop, etc.) and, if necessary to distinguish it from other devices of the same type, description of that device (e.g. Pink cellphone, Toshiba laptop, etc,);
e) Only if **examination is resultant, password**(s) and any relevant security protection details (the password should be noted on a separate paper until it is determined the examination was resultant);
f) Steps taken to **disable network connectivity**;
g) **Areas examined** on the device (e.g. gallery, documents, etc.)
h) **Documents of interest** (e.g. note a description of a photo suspected of being child pornography or note the name of a document with suspected evidence of IRPA misrepresentation);
i) **If the rationale for your examination changes** as new indicators arise (e.g. was for IRPA purposes but indicators of prohibited material have arisen) note that change in rationale;
j) If relevant, the **traveller's demeanor** and any communication with respect to the device and its contents;
k) If **assistance was obtained**, note the individuals involved
l) If any **facilitative technology** was used by CBSA experts (e.g. DFU provided unlocking services), note that; and
m) If examination is resultant, note the **next steps taken**.

SHORTENED LIST:

a) **Local date and time**
b) **Indicators**
c) **Program legislation rationale**
d) **Type of device**
e) **Only if examination is resultant, password**(s)
f) **Disable network connectivity**;
g) **Areas examined**
h) **Documents of interest**
i) **If the rationale for your examination changes**
j) **Traveller's demeanor**
k) **If assistance was obtained**
l) **Facilitative technology**
m) **Next steps taken**.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Interim Measures in Alberta and Ontario
Example of where the application of the *Customs Act* 99(1)(e) does not apply

Incorrect Application: 99(1)(e) does not apply in the below scenario as the personal digital device examination is for evidence of a contravention on the device as opposed to goods on the device that themselves are being imported in contravention of CBSA program legislation.

Example: A returning Canadian traveller is referred to secondary to have their declaration verified. In secondary, the officer reviews the traveller's declaration and has doubts about the value and accuracy of the declaration.

Due to the multiplicity of indicators observed, the officer believes that the examination of the traveller's PDD may uncover evidence of an incorrect declaration/undervaluation of goods. After enabling airplane mode and ensuring network connectivity is disabled, the officer opens the email inbox of the traveller's cellular phone, and uncovers electronic receipts that show the true number and value of the goods imported by the traveller.

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Personal Digital Device Examinations in Alberta and Ontario – as of April 29, 2022

Customs Act para. 99(1)(e) Examination of Goods

- Officer suspects on **reasonable grounds** that contravention in respect of any goods has occurred
- Officer can examine the goods and open or cause to be opened any package or container

Reasonable Grounds to Suspect (RGTS)

- Must be factually and objectively grounded
- Higher than mere suspicion but falls short of reasonable grounds to believe that a contravention has occurred
- Indicates the possibility of a contravention of CBSA program legislation

RGTS and Personal Digital Device Examinations

Personal Digital Device (PDD) examinations can be initiated under 99(1)(e) if an officer has an objective and reliable basis to suspect that the device contains contraband. The suspicion must be:

Does it pass the **LIP** test?

- **Localized** – specific to the border at the time of crossing (**PDD examination must occur at port of entry**)
- **Individualized** – specific to a traveller's PDD (who has been subject to a progressive exam)
- **Particularized** – specific to a contravention with respect to digital goods/material (i.e., goods considered contraband)

CONTRABAND

- An officer can initiate a PDD examination under 99(1)(e) if they suspect on reasonable grounds that the **good itself is prohibited or that it contains prohibited material** (e.g., videos or images of suspected child pornography)

EVIDENCE OF CONTRAVENTION

- An officer **cannot** rely on 99(1)(e) to examine **a PDD for evidence of a contravention** of CBSA program legislation related to other accompanying physical goods (e.g., receipt proving undervaluation or messages indicating hidden contraband not on the device)

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Personal Digital Device Examinations in Alberta and Ontario – Process Flow for 99(1)(e)

Referral to secondary ; appropriate level of questioning and baggage examination has been conducted

Do indicators remain that have not yet been negated and a PDD is present?

NO → No PDD examination conducted

YES

Is the suscipion linked to a contravention (prohibited document) on an accompanying PDD?

NO → No PDD examination conducted

YES

Are indicators factual and objective to sufficiently meet a RGTS threshold?

NO → No PDD examination conducted

YES

Is the suspicion sufficiently particularized that a traveller should be detained**

NO → No PDD examination conducted

YES

Officers should afford s. 10 *Charter* rights prior to asking for an access code or conducting a PDD exam

- Detain traveller
- Advise of their rights, caution, & afford them the opportunity to contact counsel

Key Policy Requirements: Supervisor Approvals and Officers Notes

- Officers must take accurate and contemporaneous notes.
- Officers must get approval from a superintendent/chief before conducting a PDD exam (pre-approval).*
- Superintendent/chief must sign-off on notes within 24 hours (post-approval).*

* Sufficient record of approval: initials, email (if viable), or officer recording name of approving supervisor in notebook.

**Detention Factors to Consider:

- Would it be more appropriate to detain the device pursuant to the *Customs Act* s. 101 (i.e., goods cannot be released) or
- Should the traveller be detained (i.e., traveller is not free to leave)?
- Would a reasonable person come to the same conclusion based on the particularized suspicion present and information available?

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Interim Measures in Alberta and Ontario
Practical Application for Section 99(1)(e) of the *Customs Act* – Child Pornography

Practical Application: If reasonable suspicion exists regarding a contravention under an Act/Regulations specific to the goods being examined: i.e. a search under section 99(1)(e) of the *Customs Act* for child pornography (CP).

Example: Officer identifies several factors pointing to the suspected importation of child pornography (CP):

These factors give the officer Reasonable Grounds to Suspect (RGTS) that a prohibited good (eg CP) is being imported on the personal digital device. The RGTS threshold has been met-and relates to a contravention in respect of digital goods on the device itself, a personal digital device examination is initiated after approval is provided by the supervisor [and after the officer affords the traveller their rights under s. 10 of the *Charter*].

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

OPERATIONAL BULLETIN: OBO-2019-055

TITLE: Implementation of the Policy on Port of Entry (POE) Examinations of Travellers' Digital Devices

Date of Issue:	Mode(s):	Target Audience:	Area of Interest:
2019-11-29	All	National	Port of Entry

Details:

- The purpose of this Operational Bulletin (OB) is to introduce the CBSA's new policy on POE Examinations Of Travellers' Digital Devices to all staff (Enforcement Manual Part 4 Chapter 16).
- The new policy expands on the previous OB (PRG-2015-31), providing more details on the procedures to be followed by all operational staff.
- The policy will go live on Monday December 2, 2019.
- The policy on POE Examinations Of Travellers' Digital Devices will provide CBSA Officers with a framework for the lawful, reasonable and progressive POE examinations of travellers' digital devices while recognizing and respecting the potential private nature of data contained within these devices.
- This policy applies to any CBSA Officer who may, as part of their duties, examine a traveller's digital device as part of a secondary examination under the *Customs Act* or the *Immigration and Refugee Protection Act* at a port of entry.
- Mandatory training is available and must be completed by all Border Services Officers (BSOs)/Superintendents/Chiefs within 3 months from the issuance of this policy. Training is recommended for anyone else whose work has a nexus to POE examinations of digital devices. (Course code: S7188-P)

Roles and Responsibilities:

- Border Services Officers (BSOs) are responsible for:
  a. BSOs working at POE must be familiar with the policy on the examination of travellers' digital goods.
  b. BSOs are responsible for taking the mandatory training on the Examination of Digital Devices

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

c. BSOs are responsible for following the guidance and directives contained within the policy on the examination of travellers' digital goods.
d. As per the policy guidance contained herein, BSOs are responsible for:
    i. remaining sensitive to the potential private nature of data stored on digital devices;
    ii. following guidance on when and how digital devices can be examined;
    iii. reporting any examinations of travellers' digital devices to CBSA Headquarters (as per OB PRG-2017-61 and per Shift Briefing Bulletin 2019-HQ-AC-05-10)
    iv. making timely and comprehensive notes whenever a traveller's digital device is examined.

- Regional Intelligence Officers (RIO) are responsible for:
    a. Familiarizing themselves with the policy on examinations of travellers' digital devices, and
    b. Remaining available to consult with other CBSA Officers who may examine travellers' digital goods, including BSOs that encounter lookouts when processing travellers, to provide additional information to the BSO that could assist the BSO in determining if a digital device examination is justified.

- Superintendents are responsible for:
    a. Familiarizing themselves with the policy on examinations of travellers' digital devices;
    b. Ensuring BSOs working in the traveller continuum familiarize themselves with the policy on examinations of travellers' digital devices; and
    c. Ensuring BSOs follow the policy guidance contained herein, including but not limited to:
        i. Not conducting digital device exams as a matter of course;
        ii. Not conducting examinations solely for the purpose of finding an offence under the Criminal Code;
        iii. Taking comprehensive and timely notes when devices are examined;
        iv. Remaining sensitive to the potential private nature of these goods; and
        v. Reporting to CBSA HQ all instances of examinations of travellers' digital devices as per PRG-2017-61 and per Shift Briefing Bulletin 2019-HQ-AC-05-10
    d. Performing periodic compliance verifications to ensure BSOs are following the policies contained herein.

- Chiefs are responsible for:
    a. Ensuring ports of entry in their jurisdiction are aware of the policy on examinations of travellers' digital goods;
    b. Ensuring BSOs in their jurisdiction have completed the requisite training on the examination of digital devices;

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

c. Ensuring Superintendents exercise due diligence in reporting instances of digital goods examinations to CBSA Headquarters as per PRG-2017-61 and per Shift Briefing Bulletin 2019-HQ-AC-05-10; and
d. Ensuring Superintendents perform periodic compliance verifications to ensure BSOs are following the policies contained herein, including note taking.

Contact Information:
Traveller Compliance Unit, Program Compliance and Outreach Division, Travellers Branch

Questions regarding this bulletin should be directed to the Traveller Compliance Unit via e-mail at: CBSA.Trav_Compliance-Conformite_voyag.ASFC@cbsa-asfc.gc.ca

Approved by:
Giovanni Matrisciano, Director Program Compliance and Outreach Division,
Traveller Programs Directorate, Travellers Branch

Effective Date: 2019-12-02	**Updated:** N/A

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

OPERATIONAL BULLETIN: OBO-2021-007

TITLE: The Use of Third Party Software at Ports of Entry

Date of Issue:	Mode(s):	Target Audience:	Area of Interest:
2021-02-12	All	All ports	National

Details:

National Headquarters (NHQ) has become aware that some ports may still be using previously issued software to examine digital devices at ports of entry (e.g. ICWhatUC, Field Search). This operational bulletin serves as a reminder that third party software **must not** be used at POEs. As per the Policy on Port of Entry Examinations of Travellers' Digital Devices, examinations that take place at ports of entry must be conducted manually and without the assistance of software/hardware. If you require assistance from the Digital Forensics Unit (DFU) when conducting a digital device examination, this should be noted in your notebook.

If third party software is available at your port (even if that software is not in use), it must be disposed of. If it is a CD or DVD proper disposal is to shred or cut up the disk into pieces. If it is in another format (e.g. flash drive) it should be given to your local Digital Forensics Investigator.

If your port has any media review laptops/toughbooks/tablets that have third party software capable of examining digital devices installed, that hardware must also be given to your local Digital Forensics Investigator.

Digital Forensic Investigators are solely responsible for the physical destruction of this technology. Ports are responsible for ensuring all such software/hardware is accounted for and disposed of properly (either by the port or by transferring to the Digital Forensic Investigator).

Actions required by BSOs:

- BSOs must be aware of and follow the policy on Port of Entry Examinations of Travellers' Digital Devices (Part 4, Chapter 16 of the Enforcement Manual) when examining digital devices
- BSOs must take the mandatory training on the examination of digital devices (course code: S7188-P)

Actions required by Superintendents/Chiefs:

- Superintendents/Chiefs must ensure no third party software is being used at their POE
- Superintendents/Chiefs must dispose of any third party software at their POE
- Superintendents/Chiefs must ensure that BSOs are following the Policy on Port of Entry Examinations of Travellers' Digital Devices (Part 4, Chapter 16 of the Enforcement Manual) when examining digital devices

References:

Policy on Port of Entry Examinations of Travellers' Digital Devices

Contact Information:

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Traveller Compliance Unit, Program Compliance Division, Travellers Policy and Programs Directorate
Travellers Branch

Questions regarding this bulletin should be directed to the Traveller Compliance Unit via e-mail at:
cbsa.trav_compliance-conformite_voyag.asfc@cbsa-asfc.gc.ca

Approved by: Marc Towaij A/Director
Program Compliance Division
Traveller Policy and Programs Directorate
Travellers Branch

Effective Date: 2021-02-12	**Updated:** N/A

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

OPERATIONAL BULLETIN: OBO-2021-023

TITLE: Changes to Notetaking Requirements in the Policy on Port of Entry Examinations of Travellers' Digital Devices

Date of Issue:	Mode(s):	Target Audience:	Area of Interest:
2021-04-08	All	All ports	National

Details:

NHQ has implemented changes to the notetaking requirements for officers when preforming digital device examinations. The results of the monthly notebook reviews of digital device examinations caused NHQ to take a closer look at what is being required from officers in the Policy on Port of Entry Examinations of Travellers' Digital Devices.

NHQ has taken the Region's comments into account which has ultimately led to these policy changes. NHQ has reduced the number of elements required to be noted for every examination, clarified the wording surrounding some of the elements and rearranged the list so it more closely follows the progression of a digital device examination. These changes are meant to clarify and streamline the notetaking process.

The updated notetaking requirements are as follows:

a) Local date and time, including the start and end time of the digital device examination;
b) Indicators observed by the officer;
c) CBSA program legislation rationale for the examination (i.e. what are the indicators pointing towards? IRPA concerns, prohibited material, etc.);
d) Type of device (e.g. Cellphone, laptop, etc.) and, if necessary to distinguish it from other devices of the same type, description of that device (e.g. Pink cellphone, Toshiba laptop, etc,);
e) Only if examination is resultant, password(s) and any relevant security protection details (the password should be noted on a separate paper until it is determined the examination was resultant);
f) Steps taken to disable network connectivity;
g) Areas examined on the device (e.g. gallery, documents, gmail, etc.)
h) Documents of interest (e.g. note a description of a photo suspected of being child pornography or note the name of a document with suspected evidence of IRPA misrepresentation);
i) If the rationale for your examination changes as new indicators arise (e.g. was for IRPA purposes but indicators of prohibited material have arisen) note that change in rationale;
j) If relevant, the traveller's demeanor and any communication with respect to the device and its contents;
k) If assistance was obtained, note the individuals involved
l) If any facilitative technology was used by CBSA experts (e.g. DFU provided unlocking services), note that; and
m) If examination is resultant, note the next steps taken.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Actions required by BSOs:

- BSOs must familiarize themselves with the new notetaking requirements in the Policy on Port of Entry Examinations of Travellers' Digital Devices

Actions required by Superintendents/Chiefs:

- Superintendents/Chiefs must familiarize themselves with the new notetaking requirements in the Policy on Port of Entry Examinations of Travellers' Digital Devices
- Superintendents/Chiefs must ensure that BSOs are following the Policy on Port of Entry Examinations of Travellers' Digital Devices (Part 4, Chapter 16 of the Enforcement Manual) when examining digital devices

References:

Policy on Port of Entry Examinations of Travellers' Digital Devices

Contact Information:

Traveller Compliance Unit, Program Compliance Division, Travellers Policy and Programs Directorate
Travellers Branch

Questions regarding this bulletin should be directed to the Traveller Compliance Unit via e-mail at:
cbsa.trav_compliance-conformite_voyag.asfc@cbsa-asfc.gc.ca

Approved by: Marc Towaij A/Director
Program Compliance Division
Traveller Policy and Programs Directorate
Travellers Branch

Effective Date: 2021-04-08	**Updated:** N/A

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

OPERATIONAL BULLETIN: OBO-2021-037

TITLE: New Measures for Conducting Digital Device Examinations

Date of Issue:	Mode(s):	Target Audience:	Area of Interest:
2021-06-08	All	All ports	National

Details:

NHQ has established new interim measures that must be complied with when examining digital devices that accompany a traveller.

Border Services Officers (BSOs) are **no longer eligible** to conduct digital device examinations if they have **not completed** the Examination of Digital Device (S7188-P) online training.

It is now **mandatory** for BSOs to receive Superintendent/Chief approval prior to conducting a digital device examination (this approval can be obtained either in person or over the phone). BSOs must be able to provide rationale to Superintendents/Chiefs as to why they will be conducting a digital device examination. For example, what indicators are present and what contravention those indicators are pointing towards. This applies to all examinations of digital devices accompanying a traveller (i.e. those performed either under the *Customs Act* or the *Immigration and Refugee Protection Act*).

Superintendents/Chiefs are not required to oversee the entire exam, however, after an examination occurs, a Superintendent/Chief must review the BSO's examination notes and ensure that the ICS entry is completed and closed. The review of BSO notes does not need to occur right away, but must be completed within 48 hrs of the examination. If the BSO's notes are insufficient upon review, the notes must be updated prior to the end of the BSO's next shift.

Further action may be taken by port management as a result of non-compliance.

Actions required by BSOs:

- BSOs must complete the Examination of Digital Device (S7188-P) online training in order to conduct digital device examinations;
- BSOs must be receive pre-approval from Superintendents/Chiefs before conducting a digital device examination; and
- BSOs must amend their examination notes if requested by a Superintendent/Chief.

Actions required by Superintendents/Chiefs:

- Superintendents/Chiefs must complete the Examination of Digital Device (S7188-P) training;

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

- Superintendents/Chiefs must ensure BSOs complete the Examination of Digital Device (S7188-P) training
- Superintendents/Chiefs must approve all digital device examinations before they occur;
- Superintendents/Chiefs must review BSO notes against the list of elements required by the policy after a digital device examination occurs (list can be found here);
- Superintendents/Chiefs must initial the BSO's notebook entry after approving; and
- Superintendents/Chiefs must ensure ICS entries are completed after a digital device examination occurs.

References:

Pocket sized notetaking guide and other job aids

Collection of Data Related to the Examinations of Travellers' Digital Devices: Reporting Requirement in the Integrated Customs System (ICS)

Changes to notetaking requirements in the Policy on Port of Entry Examinations of Travellers' Digital Devices

Reminder: Examination of Digital Devices

Enforcement Manual Part 4, Chapter 16

Contact Information:

Traveller Compliance Unit, Program Compliance Division, Travellers Policy and Programs Directorate Travellers Branch

Questions regarding this bulletin should be directed to your Regional Program Officer (RPO).

If RPOs need further support, they can contact the Traveller Compliance Unit via e-mail at: **cbsa.trav_compliance-conformite_voyag.asfc@cbsa-asfc.gc.ca**

Approved by: Marc Towaij, Director
Program Compliance Division
Travellers Policy and Programs Directorate
Travellers Branch

Effective Date: 2021-06-08	**Updated:** N/A

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

OPERATIONAL BULLETIN: OBO-2021-041

Update to the use of IRPA s.16 for the examination of digital devices at ports of entry

Date of Issue:	Mode(s):	Target Audience:	Area of Interest:
2021-06-29	All	All ports in Alberta	All modes

Details:

THIS OPERATIONAL BULLETIN ONLY APPLIES TO DIGITAL DEVICE EXAMINATIONS CONDUCTED IN ALBERTA UNTIL FURTHER NOTICE

BSOs in other parts of the country should continue to follow the instructions in Part 4 Chapter 16 of the Enforcement Manual, including reaching a threshold of a multiplicity of indicators before beginning an examination of a digital device and articulating their CBSA program rationale for beginning and continuing that device examination.

As a result of the recent Alberta Court of Appeal ruling in *R v. Al Askari* 2021 ABCA 204, prior to relying on section 16 of the *Immigration and Refugee Protection Act* (IRPA) to initiate an examination of a digital device at a port of entry, border services officers (BSOs) must have a **reasonable suspicion** relating to **specified regulatory purposes** under s.16(3) of IRPA.

Specified IRPA 16(3) Regulatory Purposes:

In order to justify a digital device examination under s.16(3) of IRPA for regulatory purposes, a BSO must have reasonable suspicion with respect to a **foreign national**'s or **permanent resident**'s 1) **identity**, 2) **admissibility**, and/or 3) other **articulable regulatory non-compliance under IRPA**.

When articulating the regulatory purpose for the examination, vague device examination purpose rationales such as "IRPA non-compliance" are too broad to fulfil the requirement to indicate the specific regulatory purpose of a digital device examination. More targeted IRPA regulatory purpose rationales linked to "identity concerns" or "inadmissibility concerns" are more defensible. These rationales must link directly to the "totality of border processing circumstances" (e.g. BSO roles and responsibilities under IRPA at the port of entry, progression of port of entry processing of the traveller, and the indicators the BSO is relying on to justify initiation and progression of their digital device examination).

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Reasonable Suspicion:

A BSO's reasonable suspicion under IRPA can develop progressively during port of entry processing of a foreign national or permanent resident but must be articulable **prior** to initiating a digital device examination under 16(3). The reasonableness of a BSO's prior suspicion under IRPA will be assessed by courts against the "totality of border processing circumstances" which includes all indicators. A BSO's reasonable suspicion with respect to identity, admissibility and/or other articulable regulatory non-compliance under s.16(3) of IRPA must be tied to indicators that are fact-based, and grounded in common sense and practical, everyday experience.

The totality of the objective facts or circumstances must be articulated in a BSO's notebook and able to withstand independent scrutiny. Mere hunches and intuition are insufficient to meet the requirement of reasonable suspicion.

Superintendents/Chiefs must consider "the totality of border processing circumstances" (including both the indicators **and** specified regulatory purpose in conjunction) to determine the reasonableness of the BSO's suspicion.

BSOs and Superintendents/Chiefs must remain cognizant that they may be called upon to explain their decision-making in a court of law in terms of their port of entry roles and responsibilities under IRPA; progression of the port of entry processing of the traveller; indicators; reasonable suspicion justification; specified IRPA 16(3) regulatory purpose rationale; and progression of the device examination.

Actions required by BSOs:

- BSOs must complete the Examination of Digital Device (S7188-P) online training in order to conduct digital device examinations
- In conjunction with this bulletin, BSOs must follow the Policy on Port of Entry Examinations of Travellers' Digital Devices (Enforcement Manual Part 4 Chapter 16)
- BSOs must seek superintendent/chief approval before conducting a digital device examination under s.16(3) of IRPA

Actions required by Superintendents/Chiefs:

- Superintendents/Chiefs must complete the Examination of Digital Device (S7188-P) training
- Superintendents/Chiefs must ensure BSOs complete the Examination of Digital Device (S7188-P) training

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

- Superintendents/Chiefs must review the indicators and rationale for a digital device examination and determine if they meet the reasonableness requirements for a s.16(3) of IRPA port of entry device examination prior to granting approval to a BSO to conduct a digital device examination

References:

- Pocket sized notetaking guide and other job aids
- New measures for conducting digital device examinations
- Reminder: Examination of Digital Devices
- Enforcement Manual Part 4, Chapter 16

Contact Information:

Traveller Compliance Unit, Program Compliance Division, Travellers Policy and Programs Directorate Travellers Branch

Questions regarding this bulletin should be directed to your Regional Program Officer (RPO).

If RPOs need further support, they can contact the Traveller Compliance Unit via e-mail at: **cbsa.trav_compliance-conformite_voyag.asfc@cbsa-asfc.gc.ca**

Approved by: Marc Towaij, Director
Program Compliance Division
Travellers Policy and Programs Directorate
Travellers Branch

Effective Date: 2021-06-29	**Updated: N/A**

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

OPERATIONAL BULLETIN: OBO-2022-027

Update on the use of ss.99(1) of the *Customs Act* for examinations of personal digital devices at ports of entry in Alberta and Ontario

Date of Issue:	Mode(s):	Target Audience:	Area of Interest:
2022-04-28	All	All ports of entry in Alberta and Ontario	All modes

Details:

****THIS OPERATIONAL BULLETIN ONLY APPLIES TO PERSONAL DIGITAL DEVICE EXAMINATIONS CONDUCTED IN ALBERTA AND ONTARIO UNTIL FURTHER NOTICE****

Officers in other parts of the country should continue to follow the instructions in Part 4 Chapter 16 of the Enforcement Manual, including having a multiplicity of indicators before beginning an examination of a personal digital device and articulating in their notebooks the CBSA program rationale for beginning and continuing that device examination.

This guidance is temporary and applies only to the use of 99(1)(e) to examine devices in Alberta and Ontario during the interim period from April 29, 2022 to passage of Bill S-7. Further guidance will be provided when Bill S-7 receives Royal Assent.

Background:

On October 29, 2020, a ruling by the Court of Appeal of Alberta (ABCA) in R v *Canfield* and R v *Townsend* (*Canfield*) found para. 99(1)(a) of the *Customs Act* to be unconstitutional in relation to the examination of personal digital devices. The cases involved two convictions from 2018 for the possession and smuggling of child pornography uncovered at the border through *Customs Act* examinations of personal digital devices.

The ABCA declared that personal digital devices would no longer fall under the definition of "goods" for purposes of para.99(1)(a) of the *Customs Act* and therefore are not subject to a no-threshold examination under para.99(1)(a). However, the Court suspended the declaration until April 28, 2022, to allow Parliament to amend the legislation.

Similarly, on April 14, 2022, the Ontario Superior Court (ONSC) also ruled in R v *Pike* and R v *Scott* (possession of child pornography cases) that personal digital device examinations are unconstitutional under para 99(1)(a) of the *Customs Act*. The Public Prosecution Service of Canada (PPSC) had requested a one-year extension in the event that the provision was found unconstitutional, which ONSC did not grant. The ONSC decided that the suspension would be co-extensive with the *Canfield* suspension and expire on April 28, 2022.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

While the Government has introduced Bill S-7 proposing amendments to the *Customs Act* to address these Court decisions, Parliament is unlikely to pass these legislative amendments before the declarations of constitutional invalidity come into effect in Alberta and Ontario on April 29, 2022. Therefore, as of April 29th 2022, personal digital devices examinations **in the provinces of Alberta and Ontario** are **no longer** permitted under para. 99(1)(a).

***Customs Act* 99(1)(e):**

Officers conducting personal digital device examinations in Alberta and Ontario must now rely on the authorities under s.99(1)(e) of the *Customs Act*. Section 99(1)(e) **must** be used in the interim until legislative amendments are finalized.

Section 99(1)(e) authorizes officers to examine goods (including conveyances) where the officer **suspects on reasonable grounds** that the *Customs Act* or any Act of Parliament administered or enforced by the officer have been or might be contravened in respect of the goods. A threshold of reasonable grounds to suspect is based on the totality of the circumstances, and requires more than a "mere suspicion". Instead, it must be based on objectively discernible facts that establish a reasonable possibility (but not probability) of a contravention in respect of the goods.

Under s.99(1)(e), a personal digital device examination must **only be initiated if** there are reasonable grounds to suspect that specific CBSA program legislation has been or might be contravened in respect to digital goods (contents) on the device itself (e.g., videos or images of suspected child pornography, hate propaganda etc.). Section 99(1)(e) does not, for example, authorize officers to look for evidence that other accompanying physical goods have been imported in contravention of CBSA program legislation (e.g., a receipt proving undervaluation or indicating undeclared goods).

The facts on which an officer will be relying to conclude that they have authority to examine personal digital devices under 99(1)(e) likely mean that the traveller would be considered detained under the charter. Officers in Alberta and Ontario relying on 99(1)(e) to conduct personal digital device exams should afford section 10 *Charter* rights prior to asking for access to the device (eg. access codes) and initiating the exam.

When conducting a *Charter* detention of the traveller, please adjust the *Customs Act* contravention detention statement from the Officer Reference Booklet as follows: "I am detaining you on suspicion that your goods fail to comply with *Customs Tariff* item 9899 and that you are attempting to import prohibited goods into Canada." When detaining a traveller officers must also read the traveller their rights and caution as set out in the Officer Reference Booklet.

As with other types of goods, in cases where officers are satisfied they have authority to examine a device under para. 99(1)(e) but must detain the device for a prolonged period of time in order to examine it (e.g., to circumvent access codes), officers can detain the device pursuant to the

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Customs Act s. 101 and permit the traveller to leave. Officers will weigh all the factors of each examination to determine when it is appropriate to take this action.

Summary of thresholds for personal digital device examinations:

Authority	Alberta and Ontario Threshold	Rest of Canada
CA 99(1)(a)	**N/A**	No threshold, internal policy of a multiplicity of indicators
CA 99(1)(e)	**Reasonable grounds to suspect**	Reasonable grounds to suspect

Job aids specific to Alberta and Ontario (guidance material will be updated as required)

Actions required by BSOs:

- BSOs must complete the Examination of Digital Device (S7188-P) online training in order to conduct personal digital device examinations;
- BSOs must follow the Policy on Port of Entry Examinations of Travellers' Digital Devices (Enforcement Manual Part 4 Chapter 16);
- BSOs must follow the policy notetaking requirements listed in paragraph 59 of the Enforcement Manual Part 4 Chapter 16, as well as follow the overarching Notetaking Policy (Enforcement Manual Part 8 Chapter 1);
- BSOs must receive pre-approval from their Superintendent/Chief prior to conducting a personal digital device examination; and,
- BSOs must update their notebooks if additional information is requested by a Superintendent/Chief.

Actions required by Superintendents/Chiefs:

- Superintendents/Chiefs must complete the Examination of Digital Device (S7188-P) training;
- Superintendents/Chiefs must ensure BSOs have completed the Examination of Digital Device (S7188-P) training;
- Superintendents/Chiefs must approve all personal digital device examinations before they occur and initial in the officer's notebook;
- Superintendents/Chiefs must review the BSO's notes against the list of elements required by the policy within 24 hours after a personal digital device examination occurs;
- Superintendents/Chiefs must ensure ICS entries are completed after a personal digital device examination occurs; and,
- Reporting summaries of personal digital device exams through existing shift reporting, and ensuring RDGs are briefed daily.

References:

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Job Aid on Reasonable Grounds to Suspect

Pocket sized notetaking guide and other job aids

New measures for conducting digital device examinations

Reminder: Examination of Digital Devices

Enforcement Manual Part 4, Chapter 16

Operational bulletin: OBO-2021-041

Contact Information:

Traveller Compliance Unit, Program Compliance Division, Travellers Policy and Programs Directorate Travellers Branch

Questions regarding this bulletin should be directed to your Regional Program Officer (RPO).

If RPOs need further support, they can contact the Traveller Compliance Unit via e-mail at: **cbsa.trav_compliance-conformite_voyag.asfc@cbsa-asfc.gc.ca**

Approved by: Marc Towaij, Director
Program Compliance Division
Travellers Policy and Programs Directorate
Travellers Branch

Effective Date: 2022-04-29	**Updated: N/A**

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Shift Briefing Bulletin

Subject :	Reminder: Examination of Digital Devices
Date :	2020-10-30

Details:

As you may be aware, on October 29, 2020 there was a ruling by the Alberta Court of Appeal in regards to the Canfield/Townsend case. This case involves two convictions from 2018 for the possession and smuggling of child pornography uncovered at the border through examinations of digital devices.

The appeal judges found that digital devices no longer fall under the definition of "goods" in the *Customs Act* and therefore are not subject to examination under s.99(1)(a). However, the court has suspended this decision for a year to allow Parliament to amend legislation or appeal the decision.

Because of the suspension of this decision, Officers are authorized to continue to conduct examinations of digital devices until further notice. However, it is extremely important to be compliant with the Policy on Port of Entry (POE) Examinations of Travellers' Digital Devices when conducting these examinations to avoid any legal and *Charter* violations.

Actions required by BSOs/Superintendents/Chiefs:

- BSOs/Superintendents/Chiefs must be familiar with the policy on the examination of travellers' digital goods
- BSOs/Superintendents/Chiefs are responsible for following the guidance and directives contained within the policy on the examination of travellers' digital goods.
- BSOs must conduct digital device examinations in compliance with the policy which includes (but not limited to):
  - Taking detailed notes;
  - Gathering a multiplicity of indicators before beginning an examination;
  - Disabling network connectivity before beginning an examination;
  - Not conducting the examination solely or primarily for the purpose of finding an offence under the *Criminal Code*; and
  - Remaining sensitive to the potential private nature of these goods.

Inquiries:

Questions regarding this bulletin should be directed to your Regional Program Officer. If additional guidance is required, the Traveller Compliance Unit can be reached via e-mail at: cbsa.trav_compliance-conformite_voyag.asfc@cbsa-asfc.gc.ca.

References:

Policy on Port of Entry Examinations of Travellers' Digital Devices

Issued by:

Marc Towaij

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

A/Director, Program Compliance Division
Travellers Policy and Programs Directorate
Travellers Branch

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Shift Briefing Bulletin

Subject :	Reminder: Examination of Digital Devices
Date :	2021-10-27

Details:

As you may be aware, on October 29, 2020 the Court of Appeal of Alberta ruled on the case of R v *Canfield* and R v *Townsend* in regards to the examination of digital devices. This case involves two convictions from 2018 for the possession and smuggling of child pornography uncovered at the border through examinations of digital devices.

In *Canfield*, the appeal judges ruled that personal digital devices no longer fall under the definition of "goods" with respect to examinations under section 99(1)(a) of the *Customs Act*. The Court suspended this decision for a year to allow Parliament time to amend legislation and this had been set to expire on October 28, 2021.

The Canada Border Services Agency submitted a request for extension on the suspension on constitutional invalidity which was heard on October 19, 2021. On October 22, 2021 a six month extension was granted by the Court of Appeal of Alberta to April 28, 2022 for Parliament to amend the *Customs Act* in order to address the Court's ruling. Therefore, personal digital device examinations are still authorized under para. 99(1)(a) provided that they are compliant with the Policy on Port of Entry (POE) Examinations of Travellers' Digital Devices.

Officers are authorized to continue conducting examinations of digital devices under para. 99(1)(a) as per the current Policy on Port of Entry (POE) Examinations of Travellers' Digital Devices until further notice. Compliance with the policy remains critical when conducting these examinations to avoid any legal and *Charter* violations.

Actions required by Border Services Officers (BSO)/Superintendents/Chiefs:

- BSOs/Superintendents/Chiefs must be familiar with and follow the guidance and directives contained within the policy on the examination of travellers' digital goods
- BSOs must seek superintendent/chief approval before conducting a digital device examination
- Superintendents/Chiefs must review the indicators and rationale for a digital device examination prior to granting approval to a BSO to conduct a digital device examination
- BSOs/Superintendents/Chiefs must complete the Examination of Digital Device (S7188-P) online training in order to conduct digital device examinations
- BSOs must conduct digital device examinations in compliance with the policy which includes (but not limited to):
    - Taking detailed notes;
    - Gathering a multiplicity of indicators before beginning an examination;
    - Disabling network connectivity before beginning an examination;
    - Not conducting the examination solely or primarily for the purpose of finding an offence under the *Criminal Code*; and,
    - Remaining sensitive to the potential private nature of these goods.

Inquiries:

Questions regarding this bulletin should be directed to your Regional Program Officer. If additional guidance is required, the Traveller Compliance Unit can be reached via e-mail at: cbsa.trav_compliance-

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

conformite_voyag.asfc@cbsa-asfc.gc.ca.

References:

Policy on Port of Entry Examinations of Travellers' Digital Devices

New measures for conducting digital device examinations

Digital Device Examination Job Aids

Issued by:

Marc Towaij
Director, Program Compliance Division
Travellers Policy and Programs Directorate
Travellers Branch

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Canada Border Services Agency | Agence des services frontaliers du Canada

Data Source: CBSA COGNOS – PSSR and TRSSR

Prepared by: Data Analytics and Performance Reporting, Travellers Branch

Extracted: 2024-05-29

Notes: Digital Device examination data from February 1, 2020 to April 30, 2024 from the Integrated Customs System (ICS).

PDD examination volumes and rates since April 29, 2022 (+comparison to prior years) - Filtered by Province/Region

a) April 29, 2022 to April 30, 2024

Region	Traveller Volumes	Digital Device Exams	Resultant Exams	Resultant Exams %
Alberta	8,642,924	44	21	47.7%
Ontario	52,856,687	266	92	34.6%
All Other	100,649,906	1,587	716	45.1%
National Total	**162,149,517**	**1,897**	**829**	**43.7%**

b) February 1, 2020 to April 28, 2022

Region	Traveller Volumes	Digital Device Exams	Resultant Exams	Resultant Exams %
Alberta	2,636,298	268	62	23.1%
Ontario	27,933,166	2,384	523	21.9%
All Other	19,489,439	2,717	800	29.4%
National Total	**50,058,903**	**5,369**	**1,385**	**25.8%**

Notes:

- *We can only provide digital device search data - with corresponding provincial breakdowns - from February 2020 forwards. As the system previously used to record this data does not have regional breakdowns.*
- *Due to some of the data in this report being pulled from manual sources, total volumes are subject to slight changes over time. Therefore, please note that these volumes may differ from other traveller reports.*
- *The data provided above provides a close approximation of total digital device exam stats. Please note that a small percentage of digital device exams are housed in a different system which does not allow for a breakdown based on exam location. For those reasons the figures above may be slightly lower than the actual counts of digital device searches.*

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Examination of Personal Digital Devices

Bottom Line: Need to introduce legislative changes regarding the examination of the contents of personal digital devices (PDD) in response to the Court of Appeal of Alberta and Ontario Superior Court's decisions that such searches are unconstitutional under the *Customs Act* (CA), para. 99(1)(a) keeping in mind the following:

- **Court's deadline of April 28, 2022 for suspension of constitutional invalidity has now passed**
- **Proposed framework balances traveller privacy with border integrity**

As legislative changes could not be ratified before the end of the suspension period, the CBSA is applying temporary mitigation measures in Alberta and Ontario until the new approach is implemented nationally under the new legislative threshold in order to avoid further enforcement gaps

R v *Canfield* and R v *Pike*

- In October 2020, the Court of Appeal of **Alberta** ruled in *Canfield* that para. 99(1)(a) of the CA, in the context of PDD examinations, is **unconstitutional as it imposes no limits on such examinations**
- Court **suspended the decision of unconstitutionality until April 28, 2022** to allow Parliament to make changes
- **Ontario** Superior Court in Pike similarly finds such exams under unconstitutional, ruling is concurrent to the timing of *Canfield*'s expiry

Why PDD Examinations Matter?

- **PDD examinations are used to screen for prohibited and harmful goods** such as child pornography and obscenity, and to look for evidence of other regulatory contraventions
- **Examinations are not conducted as a matter of course**, however the **resultant rate** is significantly higher than other types of examinations at around **27%** compared to less than 4% for other no threshold exams

Legislative Proposal

Canada Border Services Agency / Agence des services frontaliers du Canada — Public Safety Canada / Sécurité publique Canada

- The CBSA & Public Safety are proposing changes to both the CA & *Preclearance Act, 2016* which includes:
  - a **new exam threshold** (reasonable general concern) required to initiate the exam;
  - a **specific purpose to differentiate border-related exams** from criminal enforcement ones;
  - **controls or limits to guide the conduct** of the exam (in regulation for CBSA)
- A **new regulation is proposed to prescribe examination controls** for PDD examinations under the CA

REASONABLE GENERAL CONCERN

- Functions like current standard of **multiplicity of indicators**
- Officers must have **reasonable and objective concern(s)** that a contravention or evidence of same exists on a PDD

Engagement Plan

- Strengthening of traveller privacy protections may track positively with the Office of the Privacy Commissioner and the travelling public
- Digital devices and privacy both sensitive issues that garner attention

Next Steps

- Regulations have been drafted; awaiting bill introduction before publication
- Updating internal policy and training material as needed

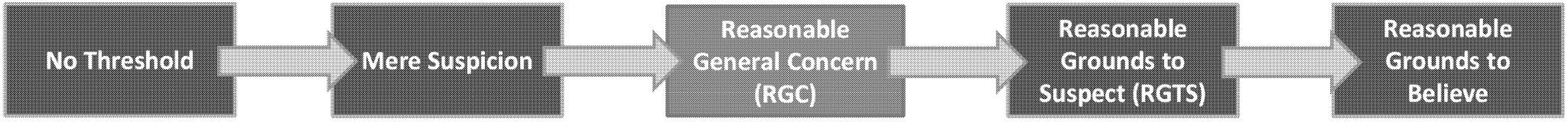
CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Personal Digital Device Examinations – *Customs Act* and *Preclearance Act,* 2016

REASONABLE GENERAL CONCERN REQUIREMENTS

New threshold states the basis and limits for the lawful examination of personal digital devices (PDD), when an officer has a **reasonable general concern** that the device may contain contraband or evidence of a contravention. The concern:

- **Must be reasonable** – more than a mere hunch and based on factors that can be objectively identified and meaningfully reviewed
- **Must be localized** – specific to the border at the time of crossing (PDD examination must occur at the border)
- **Must be case-specific** – based on the constellation of factors relating to a specific traveller or device
- **May be non-particularized** – no precise contravention need be identified



UNIQUE BORDER CONTEXT

- The border presents a unique environment with a reduced expectation of privacy in comparison to a domestic law enforcement environment
- Officers must make assessments and decisions based on limited information, timeframes, and available evidence, as only the traveller and the accompanying goods are available to question/examine

CURRENT CBSA POLICY

A PDD examination can occur if:

- There is a multiplicity of indicators suggesting a contravention or evidence a contravention of CBSA program legislation may be found on the device
- An officer has concern(s) that contravention or evidence of one (related to importation or exportation of goods) exists on a PDD

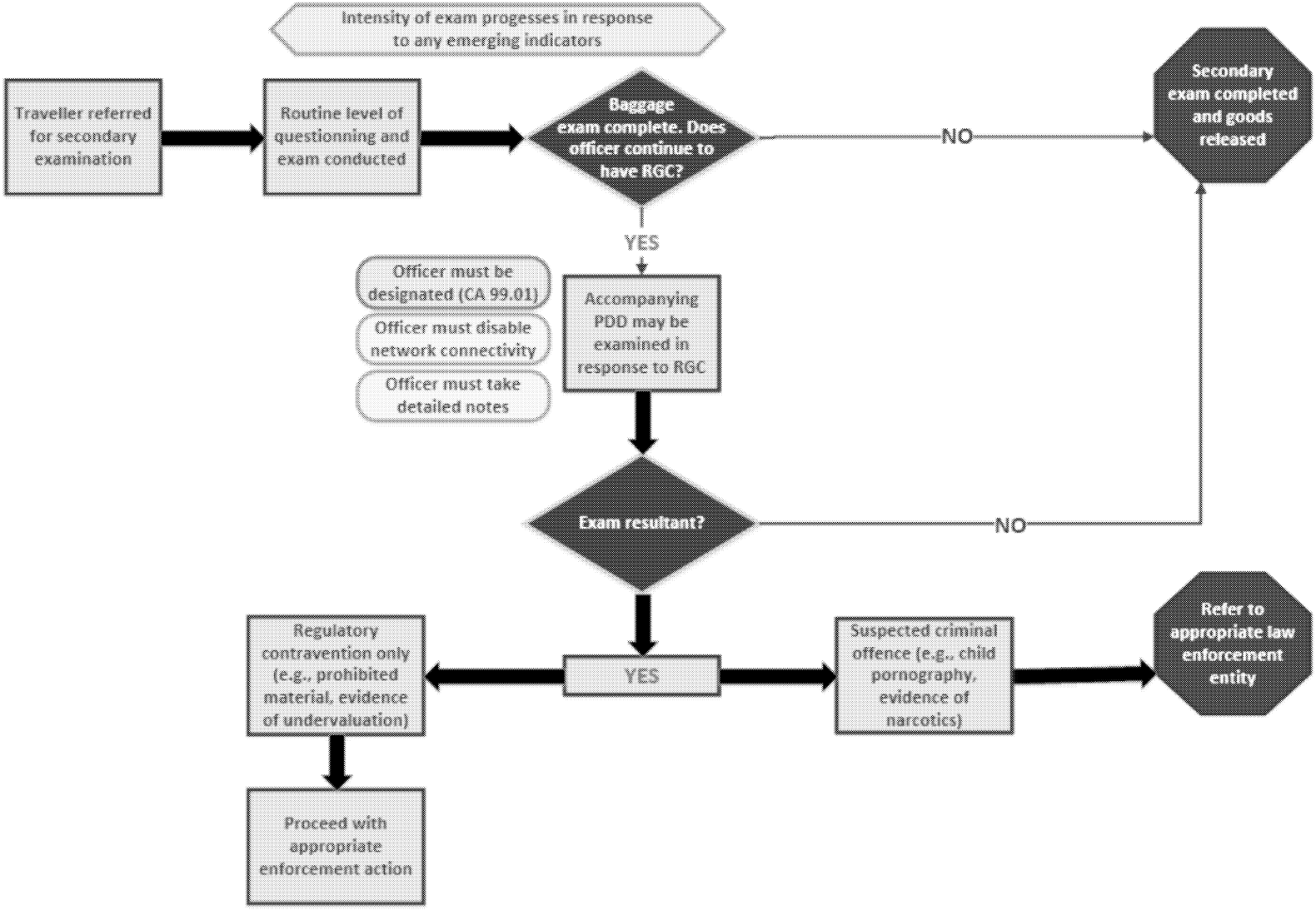
RGC VS. RGTS

- RGC is more conducive to routine border examinations whereas RGTS is primarily used at the border for personal searches which are considered more intrusive
- Risk that RGTS may require particularized suspicion; if applied to PDD exams, it could lead to weakened border control and integrity (given the need to articulate indicators of a specific contravention)

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

Reasonable General Concern

Process flow demonstrating progression of CBSA examinations involving a personal digital device



Recent Statistics (2021)

No. of travellers:	18.97M
No. of PDDs examined:	1,794
Examination rate:	0.009%
No. of resultant exams:	502
Resultant rate:	27.98%

Legend
PDD – personal digital device
RGC – reasonable general concern

Legislative requirement | Regulatory requirement

CBSA - Released under the Access to Information Act
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information

KEY STATISTICS

BILL S-7: *AN ACT TO AMEND THE CUSTOMS ACT AND THE PRECLEARANCE ACT, 2016*

Canada Border Services Agency (CBSA)

Examinations

- The CBSA does not conduct examinations of personal digital devices as a matter of course
- On average, only 1 exam is conducted per 10,000 travellers processed

Time Period	Total Number of Travellers	Total Number of Exams	Examination Rate
2020	26,712,576	4174	0.016%
2021	18,974,809	1794	0.009%
January 2022	2,109,291	111	0.005%
February 2022	2,076,958	100	0.005%
March 2022	3,447,754	77	0.002%
April 2022	4,619,699	77	0.002%

Examination statistics are from January 30, 2020 to April 30, 2022.

Results

Time Period	Total Number of Exams	Total Number of Resultants	Resultant Rate
2020	4174	1095	26%
2021	1794	502	28%
January 2022	111	52	47%
February 2022	100	25	25%
March 2022	77	24	31%
April 2022	77	32	41%

Resultant describes an examination where a customs- or immigration- related contravention or offence has been uncovered and can include enforcement actions under both the *Customs Act* and the *Immigration and Refugee Protection Act*

Preclearance

- The below table outlines the total number of travellers, originating from or transiting through Canada into the United States (US) and underwent US preclearance processing in a Canadian airport
- All figures have been provided by United States Customs and Border Protection.

Time Period (calendar year)	Total Travellers
2018	16,336,189
2019	16,788,927
2020	3,597,162
2021	2,661,303
2022 (as of March 27, 2022)	1,432,343