**OPERATIONAL BULLETIN: PRG-2015-31**

**TITLE: Examination of Digital Devices and Media at the Port of Entry – Guidelines**

| Date of Issue: | Mode(s): | Target Audience: | Area of Interest: |
|---|---|---|---|
| 2015-06-30 | All | National | Port of Entry |

**Details:**

- The purpose of this operational bulletin is to provide guidance on a CBSA officer's authority to examine digital devices or media at ports of entry. Clarification will be provided on when such examinations should and can be performed, and will explain limitations to these authorities.

**Authorities:**

- Digital devices and media, along with digital documents and software, continue to be classified as 'goods' in the context of the border. A CBSA officer's authority to examine goods is specified under the *Customs Act* and the *Immigration and Refugee Protection Act* (IRPA).
- Paragraph 99(1)(*a*) of the *Customs Act* provides CBSA officers with the legislative authority to examine goods, including digital devices and media, for customs purposes only. Although there is no defined threshold for grounds to examine such devices, CBSA's current policy is that such examinations should not be conducted as a matter of routine; they may only be conducted if there is a multiplicity of indicators that evidence of contraventions may be found on the digital device or media.
- Subsection 139(1) of the IRPA allows for the search of digital devices and media at the ports of entry where there are reasonable grounds to believe that the person has not revealed their identity or has hidden, on or about their person, documents that are relevant to their admissibility; or has committed, or possesses documents that may be used in the commission of people smuggling, human trafficking, or document fraud. The purpose of this search must be confined to identifying the person, finding documents relevant to admissibility or that may be used in the specified offences, or finding evidence of the specified offences.
- Examination of digital devices and media must **always** be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation

that governs the cross-border movement of people and goods, plants and animals. 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. Officers must be able to explain their reasoning for examining the device, and how each type of information, computer/device program and/or application they examine may reasonably be expected to confirm or refute those concerns. The officer's notes shall clearly articulate the types of data they examined, and their reason for doing so.

**Actions required by CBSA officers:**

- Where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods, officers are authorized to conduct progressive examinations of digital devices and media for evidence of contraventions or to support allegations.
- Evidence may include, for example, electronic receipts for goods; information that refers to the acquisition or origin of the goods; or information that may afford evidence of a contravention to CBSA-mandated legislation that governs the admissibility of people and goods, plants and animals into and out of Canada. Such evidence may, for example, uncover the following: a confirmation of identity; receipts and invoices for imported goods; contraband smuggling; or, the importation of obscenity, hate propaganda or child pornography.
- Where the identity or admissibility of a traveller is in question, officers are justified in performing examinations of digital devices and media to discover the traveller's true identity, evidence of false identities, or other documentary evidence pertaining to admissibility.
- Where evidence of a criminal offence is discovered during the examination process, officers must be cognisant of where the regulatory examination crosses over to the realm of a criminal investigation. Officers must determine on a case-by-case basis, through consultation with their supervisor, whether or not to continue the regulatory examination and identify any possible impacts on potential criminal investigations.
- Officers must follow the CBSA Enforcement Manual Part 9 instructions on securing evidence and on referrals to Criminal Investigations, as well as following regional requirements for referrals to Inland Enforcement or Intelligence.
- CBSA officers shall conduct examinations of digital devices and media with as much respect for the traveller's privacy as possible, considering that these examinations are usually more personal in nature than baggage examinations.

*Examination Progression*

- Prior to examination of digital devices and media, and where possible, CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) to limit the ability of the device to connect to remote hosts or services. This will reduce the possibility of triggering remote wiping software; inadvertently accessing the Internet or other data stored externally; or changing version numbers or dates.
- Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators.
- CBSA officers shall only examine what is stored within the device. Officers are not to read emails on digital devices and media unless the information is already downloaded and has been opened (usually marked as read).
- CBSA officers shall notate in their notebooks the indicators that led to the progressive search of the digital device or media; what areas of the device or media were accessed during the search; and why. This is to protect both the integrity of the information within the digital device and the officer.

*Passwords and Enforcement*

- With the exception of devices that are biometrically (i.e. fingerprint) protected, CBSA officers shall not allow a traveller to input a password into a digital device or media themselves. This practice reduces the risk of any contents being altered and allows for the continuity of evidence.
- In instances where access to digital devices and media are password protected, officers are to request the password to access the device and record it, as well as any alternate passwords provided, in their officer notebook.
- In cases where the device is biometrically protected, CBSA officers may allow the traveller to input the biometric information while the officer monitors and controls the device (for example, the officer may hold the device while the traveller allows the device to read their fingerprint). Should the CBSA officer find information that provides evidence of a contravention, they should then deactivate the password protection on the device or media.
- Passwords are not to be sought to gain access to any type of account (including any social, professional, corporate, or user accounts), files or information that might potentially be stored remotely or on-line. CBSA officers may only request and make note of passwords required to gain access to information or files if the information or file is known or suspected to exist within the digital device or media being examined.
- Conversely, a traveller may voluntarily provide information and passwords to access external data in certain circumstances in order to show compliance;

CBSA officers should advise travellers that they are not required to access or provide external information, but may voluntarily choose to do so. The login information or password shall not be compelled or recorded in these cases.

- If a traveller refuses to provide a password to allow examination of the digital device, media or the documents contained therein, or if there are technical difficulties that prevent a CBSA officer from examining the digital device or media, the device or media may be detained by the CBSA officer under the authority of Section 101 of the *Customs Act*, on the form K26, *Notice of Detention*, for examination by a CBSA expert trained in digital forensic examinations. For IRPA-related examinations, the device or media may be detained under the authority of subsection 140 (1) of the IRPA on the form IMM5265.
- Until further instructions are issued, CBSA officers shall not arrest a traveller for hindering (Section 153.1 of the *Customs Act*) or for obstruction (paragraph 129(1)(d) of IRPA) solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings.
- At the conclusion of a non-resultant examination, the traveller shall be advised that though their password will be protected in accordance with privacy laws, they may nonetheless change it if they wish to do so.

**Contact Information:**

Program Compliance and Outreach Division, Traveller Programs Directorate

If you have any further questions, please forward them through the regional Corporate and Program Services Divisions, which (if required) will then send an email to the Port of Entry Operations' generic inbox: CBSA-ASFC_Ops_Travellers-Voyageurs.

**Approved by:** Barry Kong, Director
Programs Compliance and Outreach Division
Traveller Programs Directorate
Programs Branch

| **Effective Date:** 2015-06-30 | **Updated:** 2017-02-28 |
|---|---|

Additional bulletins: http://atlas/ob-dgo/bso-asf/bulletin/index_eng.asp