(1)

Policy Fact Sheet

SUBJECT: Search of laptop computers

QUESTION/ISSUE:

Can a customs officer search a laptop for the purpose of looking for evidence of prohibited material/child pornography?

POLICY:

A laptop can be examined for contraband the same as any other goods. This would include opening the laptop, turning it on and perhaps calling up a few files (this is like opening a briefcase and flipping through files). To actually review the contents of each computer file is beyond a routine secondary exam and should be supported with the officer's articulatable reasons to take the exam to a higher level. The rationale that applies to laptops is consistent with that applied to Palm Pilots and journals (written or electronic).

Caution: If an officer has reasonable grounds to suspect the contents of a laptop contains child pornography, someone qualified to do a proper search of the system should be contacted. (Similar to what an officer does now when there is a question concerning the value of jewellery – it is sent out for appraisal). The officer can have reasonable grounds to suspect, but needs to rely on the technical skill provided by knowledgeable person.

Note: When conducting any search, it is critical to keep in mind Section 8 of the *Canadian Charter of Rights and Freedoms,* which states:

"Everyone has the right to be secure against unreasonable search or seizure."

REFERENCE:

1) Section 99. (1) of the *Customs Act* states:

An officer may:

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

2) Section 9899.00.00 of the *Customs Tariff* identifies photographic film, video or other visual representations, including those made by mechanical or electronic means that are child pornography within the meaning of Section 163.1 of the *Criminal Code*.

It is reasonable to ascertain that the "other visual representations" extends to electronically stored data which may be intelligible to humans such as may be contained on a computer's hard drive or on a computer diskette.

FILE: 5083-18.03 Customs Process/Examinations (Goods & Conveyances)

Windsor-St.Clair
Criminal Investigations Division
Computer Search and Evidence Recovery Procedures

The following procedures are created to define the Computer Search and Evidence Recovery (CSER) process.

1. Access to CSER Evidence

Admittance to the CSER evidence room will only be by security card profiles granted to persons authorized to have access to this evidence.

2. Use of CSER Evidence Room Cabinet

The CSER evidence room "Dasco" cabinet is to be used only for the short-term storage of goods pending the completion of an investigation or court proceeding. Only goods subject to the CSER process shall be stored in the CSER evidence cabinet.

All child pornography evidence shall be locked in the "Dasco" cabinet. Goods from no more than one case file shall be kept in each compartment.

3. Key Control

Keys will be numbered to correspond to individual lockers.

For lockers containing evidence,

When evidence is removed from the locker for its final disposition, the key will be returned

4. Evidence Control

A K129 Exhibit Control form will be used for all transfers of evidence within CBSA custody, including to and from the CSER specialist. A signed copy of the K129 shall be placed in the case file.

In all cases, the relevant CBSA forms (E650, E352, K19S, K19, K24, K27, K129, etc.) are to be cross-referenced to create an audit trail.

All evidence transferred to outside agencies will also be documented on a form K129. The K129 is to be endorsed to indicate that the goods must be returned to the CBSA at the conclusion of the court proceedings.

All used envelopes or evidence bags should be retained, either with the goods or on file, to prove chain of custody.

5. CSER Evidence Room Log

The CSER evidence room log is to be kept in an electronic format

All access to the CSER evidence cabinet must be logged by an entry in the CSER electronic evidence logbook.

It is imperative that the CIIMS file number and officer's name and badge number be placed in the logbook in order to facilitate the identification of goods and verification of their status.

6. Disposition of Goods

Upon completion of an investigation or court proceeding, goods authorised for return to their owner shall be processed according to the applicable section of the Customs Act or Criminal Code.

Goods deemed as forfeit under the Customs Act or by court order shall be transferred to the Queen's Warehouse for disposal.

Forfeit computer hard drives and electronic storage devices containing child pornography and other prohibited material shall be destroyed by drilling holes into electronic media or disks (CDs, DVDs, etc.) and subsequently ensuring that they are no longer capable of being played as per EN Manual Part 2, Chapter 8, and S. 42. This shall be done under observation of the CSER specialist.

7. Inventory of CSER Equipment

An inventory of the equipment used in the CSER process shall be maintained and updated on an annual basis by the CSER specialist.

8. Role of the Computer Search and Evidence Recovery (CSER) Specialist

- Provide technical expertise, forensically examine and extract evidence from electronic devices for CBSA Criminal Investigations.
- Provide technical expertise, forensically examine and extract evidence from electronic devices for CBSA Port of Entry enforcement actions.
- Assist Law Enforcement Agencies in combined CBSA Joint Forces Operations by providing technical expertise, forensically examining and extract evidence from electronic devices.
- Assist Law Enforcement Agencies by providing technical expertise, forensically examining and extract evidence from electronic devices.
- Assist Foreign Law Enforcement Agencies with forensic reports and analysis of electronic data, relating to offences identified in their jurisdiction, resulting from CBSA enforcement actions dealing with their nationals.
- Prepare forensic reports for "Disclosure" in criminal proceedings.
- Provide expert witness testimony during criminal proceedings.

9. Duties of the Computer Search and Evidence Recovery (CSER) Specialist

1. Criminal Investigations of mandated CBSA Criminal Investigations Division related legislation offences outside the port of entry. (i.e. Customs Act, IRPA)

2. Criminal Investigation of mandated CBSA Criminal Investigations Division related legislation for offences uncovered at the port of entry (i.e. Customs Act, IRPA) not including child pornography.

3. Criminal Investigation of mandated CBSA Criminal Investigations Division related legislation for offences dealing with prohibited goods (mainly child pornography) uncovered at the port of entry.

4. Assist Intelligence Operations relating to CBSA related legislation offences.

5. Assist Intelligence Operations relating to combined Joint Forces Operations with other law enforcement agencies.

6. Assist local law enforcement agencies with technical expertise processed by the CSER specialist for non-CBSA related enforcement actions.

7. Assist foreign law enforcement agencies with technical expertise processed by the CSER specialist for non-CBSA related enforcement actions.

8. Provide and assist other Regional CBSA CID units with CSER services for multiple location search warrant executions.

10. Computer Search and Evidence Recovery (CSER) Specialist Scenarios

Scenario 1:

Criminal Investigations of mandated CBSA Criminal Investigations Division related legislation offences outside the port of entry. (i.e. Customs Act, IRPA)

Assists the Investigator with "Information To Obtain" (ITO) information and Search Warrant wording.

Attend the execution of the search, examine and identify electronic evidence to be seized.

Investigator prepares "Request for Laboratory Examination" form outlining specific evidence needed for his/her investigation. Investigator prepares K129 Evidence Control form.

CSER takes control of seized electronic evidence for analysis on K129.

CSER documents evidence in Intake Log.

CSER reviews and meets with Investigator to review "Request for Laboratory Examination" form.

CSER forensically creates two (2) mirror copies of the electronic media.

CSER transfers custody of electronic devices back to Investigator on K129.

CSER forensically processes the mirror copy with appropriate analysis tools.

CSER interrogates the mirror copy for specific information based on meeting with Investigator.

CSER meets with Investigator to discuss findings and further guidance.

CSER re-interrogates the mirror copy based on meeting with Investigator.

CSER prepares report and burns to compact disk. If needed, prints out report.

CSER provides expert witness testimony during criminal proceedings.

Involvement concluded.

Scenario 2:

Criminal Investigation of mandated CBSA Criminal Investigations Division related legislation for offences uncovered at the port of entry. (i.e. Customs Act, IRPA) not including child pornography.

Investigator prepares "Request for Laboratory Examination" form outlining specific evidence needed for his/her investigation. Investigator prepares K129 Evidence Control form.

CSER takes control of seized electronic evidence for analysis on K129.

CSER documents evidence in Intake Log.

CSER reviews and meets with Investigator to review "Request for Examination Form".

CSER forensically creates two (2) mirror copies of the electronic media.

CSER transfers custody of electronic devices back to Investigator on K129.

CSER forensically processes the mirror copy with appropriate analysis tools.

CSER interrogates the mirror copy for specific information based on meeting with Investigator.

CSER meets with Investigator to discuss findings and further guidance.

CSER re-interrogates the mirror copy based on meeting with Investigator.

CSER prepares report and burns to compact disk. If needed, prints out report.

CSER provides expert witness testimony during criminal proceedings.

Involvement concluded.

Scenario 3:

Criminal Investigation of mandated CBSA Criminal Investigations Division related legislation for offences dealing with prohibited goods (mainly child pornography) uncovered at the port of entry.

CSER is called to the Port of Entry by an Investigator to forensically examine electronic devices suspected of containing Child Pornography.

CSER documents device details, meets with POE Border Officer to discuss his/her findings and prepares the electronic device for examination.

CSER examines electronic device and establishes if Child Pornography is present and reports findings to the Investigator. If Child Pornography is found, CSER will document his/her findings and capture selected images to be burned to compact disk for transfer to appropriate local law enforcement agency for their consideration to take action under the Criminal Code of Canada.

Investigator prepares K129 Evidence Control form.

Investigator prepares "Request for Laboratory Examination" form outlining specific evidence needed for his/her investigation.

CSER takes control of seized electronic evidence for analysis on K129.

CSER documents evidence in Intake Log.

CSER reviews and meets with Investigator to review "Request for Examination Form".

CSER forensically creates two (2) mirror copies of the electronic media.

CSER secures electronic media in special evidence locker for Child Pornography.

CSER forensically processes the mirror copy with appropriate analysis tools.

CSER interrogates the mirror copy for specific information based on meeting with Investigator.

CSER meets with Investigator to discuss findings and further guidance.

CSER re-interrogates the mirror copy based on meeting with Investigator.

CSER prepares report and burns to compact disk. If needed, prints out report.

CSER prepares forensic report for disclosure purposes.

CSER maintains control of electronic media until criminal proceedings are concluded.

At the conclusion of criminal proceedings, CSER transfers custody of electronic devices back to Investigator (K129) for destruction in an approved manner.

Involvement concluded.

Scenario 4:

Assist Intelligence Operations relating to CBSA related legislation offences.

Intelligence Officer (IO) prepares "Request for Laboratory Examination" form outlining specific evidence needed for his/her investigation. Intelligence Officer prepares K129 Evidence Control form.

CSER takes control of seized electronic evidence for analysis on K129.

CSER documents evidence in Intake Log.

CSER reviews and meets with Intelligence Officer to review "Request for Examination Form".

CSER forensically creates two (2) mirror copies of the electronic media.

CSER transfers custody of electronic devices back to Intelligence Officer on K129.

CSER forensically processes the mirror copy with appropriate analysis tools.

CSER interrogates the mirror copy for specific information based on meeting with Intelligence Officer.

CSER meets with Investigator to discuss findings and further guidance.

CSER re-interrogates the mirror copy based on meeting with Intelligence Officer.

CSER prepares report and burns to compact disk. If needed, prints out report.

CSER provides expert witness testimony during criminal proceedings.

Involvement concluded.

Scenario 5:

Assist Intelligence Operations relating to combined Joint Forces Operations with other law enforcement agencies.

Intelligence Officer (IO) prepares "Request for Laboratory Examination" form outlining specific evidence needed for his/her investigation. Intelligence Officer prepares K129 Evidence Control form.

CSER takes control of seized electronic evidence for analysis on K129.

CSER documents evidence in Intake Log.

CSER reviews and meets with Intelligence Officer to review "Request for Examination Form".

CSER forensically creates two (2) mirror copies of the electronic media.

CSER transfers custody of electronic devices back to Intelligence Officer onK129.

CSER forensically processes the mirror copy with various analysis tools.

CSER interrogates the mirror copy for specific information based on meeting with Intelligence Officer.

CSER meets with Intelligence Officer to discuss findings and further guidance.

CSER re-interrogates the mirror copy based on meeting with Intelligence Officer.

CSER prepares report and burns to compact disk. If needed, prints out report.

CSER prepares Will Say document for criminal proceedings.

CSER provides expert witness testimony during criminal proceedings.

Involvement concluded.

Scenario 6:

Assist local law enforcement agencies with technical expertise provided by the CSER specialist for non-CBSA related enforcement actions.

Law Enforcement Agency Investigator prepares "Request for Laboratory Examination" form outlining specific evidence needed for his/her investigation. CSER prepares K129 Evidence Control form.

CSER takes control of seized electronic evidence for analysis on K129.

CSER documents evidence in Intake Log.

CSER reviews and meets with LE Investigator to review "Request for Laboratory Examination" form.

CSER forensically creates two (2) mirror copies of the electronic media.

CSER transfers custody of electronic devices back to LE Investigator (K129).

CSER forensically processes the mirror copy with appropriate analysis tools.

CSER interrogates the mirror copy for specific information based on meeting with Investigator.

CSER meets with Investigator to discuss findings and further guidance.

CSER re-interrogates the mirror copy based on meeting with Investigator.

CSER prepares report and burns to compact disk. If needed, prints out report.

CSER prepares Will Say document for criminal proceedings.

CSER provides expert witness testimony during criminal proceedings.

Involvement concluded.

Scenario 7:

Assist foreign law enforcement agencies with technical expertise provided by the CSER specialist for non-CBSA related enforcement actions.

Foreign Law Enforcement Agency Investigator prepares "Request for Laboratory Examination" form outlining specific evidence needed for his/her investigation. CSER prepares K129 Evidence Control form.

CSER takes control of seized electronic evidence for analysis on K129.

CSER documents evidence in Intake Log.

CSER reviews and meets with FLE Investigator to review "Request for Laboratory Examination" form".

CSER forensically creates two (2) mirror copies of the electronic media.

CSER transfers custody of electronic devices back to FLE Investigator on K129.

CSER forensically processes the mirror copy with appropriate analysis tools.

CSER interrogates the mirror copy for specific information based on meeting with Investigator.

CSER meets with Investigator to discuss findings and further guidance.

CSER re-interrogates the mirror copy based on meeting with Investigator.

CSER prepares report and burns to compact disk. If needed, prints out report.

CSER prepares Will Say document for criminal proceedings.

CSER provides expert witness testimony during criminal proceedings.

Involvement concluded.

Scenario 8:

Provide and assist other Regional CBSA CID units with CSER services for multiple location search warrant executions.

Part I

Attend search warrant briefing and meet with Search Team members and provide expert information concerning electronic evidence.

Attend the execution of the search, examine and identify electronic evidence to be seized.

Document electronic devices to be seized for entry the Report to a Justice

Prepare search notes and advise lead investigator of findings.

Part II

If requested to provide forensics processing and analytical services concerning seize electronic devices.

Have Lead Investigator prepares "Request for Laboratory Examination" form outlining specific evidence needed for his/her investigation. Investigator prepares K129 Evidence Control form.

CSER takes control of seized electronic evidence for analysis on K129.

CSER documents evidence in Intake Log.

CSER reviews and meets with Investigator to review "Request for Laboratory Examination" form .

CSER forensically creates two (2) mirror copies of electronic media.

CSER transfers custody of electronic devices back to Investigator (K129).

CSER forensically processes mirror copy with various analysis tools.

CSER interrogates mirror copy for specific information based on meeting with Investigator.

CSER meets with Investigator to discuss findings and further guidance.

CSER re-interrogates mirror copy based on meeting with Investigator.

CSER prepares report and burns to compact disk. If needed, prints out report.

CSER provides expert witness testimony during criminal proceedings.

Involvement concluded.

11. Appendices

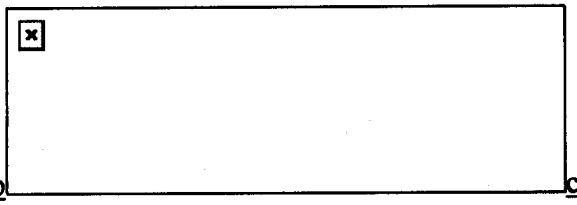
A K129 Exhibit Control Document

B Computer Forensics Lab request for Laboratory Examination

Computer Search & Evidence Recovery (CSER)

The CBSA's Investigations Division makes use of computer forensics to identify, recover and safeguard electronic evidence stored in digital media. This function has existed within Customs Investigations as the *Computer Search and Evidence Recovery (CSER)* program for many years. The need for an electronic media search and evidence recovery capability has grown with the evolution of the Information Age. In a "virtual" electronic data world, traditional enforcement techniques are not as effective against technology-literate criminals.

The principal objective of the CSER program is to provide computer and electronic media expertise to support Investigations' search warrant activities. The CSER program is critical to the Investigator's prime objective of gathering evidence to support criminal charges. Since electronic evidence is subject to the same legal requirements as "hardcopy" evidence, specific techniques to search, secure and preserve the evidentiary value is required.



content_top content_top

What Services CSERS Provide

Pre-Search Warrant

Search Warrant

Post Search Warrant

Computer Search & Evidence Recovery Specialists *(CSERS)* can forensically analyze a computer system and electronic media and retrieve a wide variety of information. This information can include, but is not limited to:

electronic documents (e.g. letters, memos, journals);

multimedia files (e.g. videos, photographs, sound recordings);

e-mail messages received and sent from the computer system;

web pages and other indicators of Internet use;

Pre-Search Warrant

Most of Investigations' regional offices have CSERS available to them. The CSERS can assist investigators in many different areas such as:

Suggest wording when writing a search warrant

Suggestions on what to search for

Technical grounds of belief and how to word these

Giving suggestions on technical investigative steps that may be required

Assessment of Search Locations

Assist with keyword search parameters

Provide briefings to search teams on electronic media evidence

Search Warrant

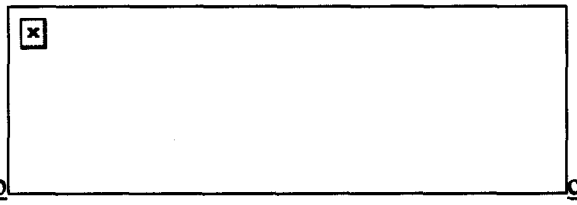
CSERS will attend search locations and essentially control the segment of the search scene involving the computer and electronic media devices. Typically, this involves conducting a preliminary site evaluation, making contact with local IT support and prioritizing the electronic media search process (more details on securing the scene are provided below).

Once the search team has secured the site, which includes having everyone moved away from computers and electronic devices, the CSERS will begin running keyword searches to locate electronic evidence. Electronic devices that yield keyword hit results will be seized by the CSERS. Depending on the volume of evidence to seize, an exact copy (called an "image") of the electronic media may be created on site. In situations where there are large volumes of evidence or complex systems, the complete electronic device with all attachments will be seized and transported back to the regional office for processing.

Post Search Warrant

Typically, the electronic evidence sought is found on the hard disk drive(s) contained within the seized computer system. The CSERS will image the entire hard disk drive, and conduct all subsequent analysis on that image. The original hard disk drive or a second hard drive image will be reinstalled in the seized computer and returned to the alleged suspect.

The analysis will include a thorough search of the entire hard disk drive and any other seized storage media for electronic evidence. The CSERS will conduct a full analysis of the seized media. Some examples of things that can be done during a forensic exam include:



content_top content_top

Securing the Scene

The investigator in charge of the case is responsible for the over-all planning of the search and its successful execution. The search planning should include determining if a CSERS would be needed to search for computerized data. In any event, a CSER officer should always be on stand-by on the day of a search in case computerized equipment is discovered.

1. Secure the Scene

   Officer safety is paramount.

   Immediately restrict access to computer(s).

   Determine if stand-alone or network computer.

   If computer is "OFF", do not turn "ON".

   Disconnect from phone line if attached to MODEM or LAN cable if connected to network.

   Interview employee present to obtain job function, software applications used, level of computer competency and use and location of other devices (e.g. laptop, PDA)

   Record and diagram computer and electronic media located at search location

2. Secure the Computer as Evidence if NO CSER is Available

   If computer is "OFF", do not turn "ON".

   If computer is "ON"

   Stand-alone computer

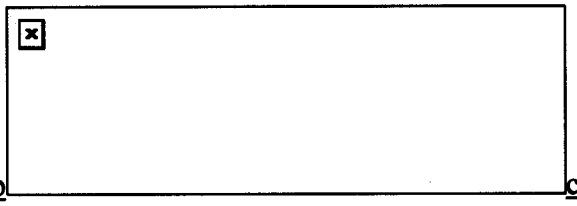
Networked or business computers

Consult a CSERS for further assistance as pulling the plug could:

Severely damage the system

Disrupt legitimate business

Create officer and department liability



content_top content_top

What to Search & Seize

For the most part, there are four possibilities:

Search the computer and print out a hard copy of particular files;

Search the computer and make an electronic copy of particular files;

Create a duplicate electronic copy of the entire storage device on-site, and then later recreate a working copy of the storage device off-site for review;

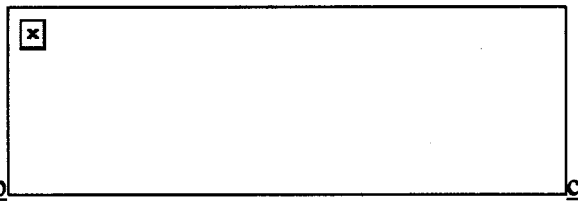
Seize the equipment, remove it from the premises, and review its contents off-site.

In general, the search strategies used will depend on the role the hardware played in the offence. As is the case with the majority of CBSA investigations, the computer hardware is a storage device that contains evidence of the crime. The hardware itself is merely a container for evidence. The purpose of searching the suspect's computer will be to recover the evidence the computer hardware happens to contain.

In other cases the computer hardware can itself be contraband, or evidence or 'fruit of the crime' itself. For example, a computer used to transmit child pornography is an instrument of the crime, as well, it is evidence of possession. Stolen computers are 'fruits of crime'.

Once on-site to execute the search, the CSERS will assess the hardware, software, and resources available to determine whether an on-site search and seizure is possible. In many cases, the search strategy will depend on the environment in which the search occurs. For example, searching and seizing information stored on computer networks of a functioning business will, in most circumstances, **not** involve seizing the business' computers, if possible. If the hardware is merely a storage device for evidence, CSERS will only seize the hardware if less disruptive alternatives are not feasible.

Section 115 of the *Customs Act* provides investigators with the authority to make copies of seized records and states that certified copies carry the same force as the originals when tended as evidence. Sections 31.1 to 31.8 of the *Canada Evidence Act* address the admissibility of electronic documents as evidence.



content_top content_top

Search Warrants

Grounds for Belief

Things to Be Searched for

Third Party Search

Solicitor/Client Privilege Claimed on Computer Seized

Microcomputer
Definition: a small digital computer based on a microprocessor and designed to be used by one person at a time; a microprocessor functions as the central processing unit of a microcomputer; a disk drive contains a microprocessor to handle the internal functions of the drive.

Grounds for Belief - Computer Search

That in the course of his/her enquiries, the Informant received information from [insert name], Investigator, an officer of the CBSA, which information the Informant does verily believe to be true, that:

(a) he/she has experience with microcomputers with respect to electronic media searches and data storage retrieval conducted by CBSA Investigations, involving computerized records and documents;

or

(a) he/she has received specialized training in microcomputers with respect to electronic media search and data storage retrieval procedures involving computerized records and documents;

and

(b) the software, documentation and electronic devices described in paragraph (b) or (c) of Things to be Searched for are required to access, retrieve and reproduce the said items described in paragraph (a) of Things to be Searched for.

Things to Be Searched for

1. Paragraph for Documents
2. For goods if applicable
3. (b) or (c) items described in paragraph (a) in electronic format; including software, documentation, electronic devices required to access, retrieve and reproduce the said items.

Third Party Search

Where a search of a third party's computerized records is required, the general practice is to restrict the seizure to copies of the information contained therein, rather than seizing the computer equipment; exceptions may apply.

Solicitor/Client Privilege Claimed on Computer Seized

Date

Office of the Sheriff (agreed upon with the lawyer)
Address
City, Province
Postal Code

Re: Personal Computer Seized Pursuant to Section 111 C.A. Search Warrant

Dear [*insert name of Sheriff here*]:

On [*insert search date*] a personal computer and contents were seized by an officer of the Canada Border Services Agency from [*insert the CBSA Investigations office doing the search*] pursuant to a search warrant issued by [*insert name of justice*].

Contents of the above-mentioned computer were the subject of a solicitor-client privilege claim pursuant to section 488.1 of the Criminal Code and the computer and contents were placed into the custody of your office on *[insert the date that the computer was put in the Sheriff's trust].*

Due to the fragile nature of electronic media, safeguards should be adhered to which exceed the needs of other physical forms of evidence. These special precautions will need to be taken to ensure that the original media is preserved and protected from both physical and electronic hazards.

The Canada Border Services Agency Investigations Division has on staff Investigators trained in computer search and evidence recovery. These Investigators (Computer Search & Evidence Recovery Specialists) have the knowledge, expertise, computer hardware and law enforcement software necessary to ensure that seized electronic evidence is preserved in its original state. CSERS are available to advise you on special storage precautions, which should be taken, with respect to the seized computer referred to above.

It is the policy of the Canada Border Services Agency to have Investigators trained in computer search & evidence recovery make a copy or backup of a seized computer hard disk, as soon as practically possible, following a search action. The copy or backup is then used:

1. to provide a copy to the person from whom it was seized should they request a copy;
2. for analysis/processing by the Canada Border Services Agency

When a backup or copy of a hard disk is made, special techniques ("safety nets") are employed to ensure that the integrity of the original media is maintained and that the electronic evidence is not altered or destroyed (only an Investigator trained in computer search and evidence recovery should access seized electronic media). In the foregoing instance, a copy of the seized hard disk was not made due to the solicitor-client privilege claim.

Given that electronic data may be easily altered or damaged, the Canada Border Services Agency requests the following, with respect to any initialization (turning the computer on), examination or copying of data or information stored on the seized personal computer, while it is under your custody:

1. Should the person from whom the computer/hard disk was seized apply under section 488.1(9) of the Criminal Code to examine documents or files on the seized hard disk, that a Canada Border Services Agency CSERS be requested to assist to install the necessary software safeguards to ensure that the documents or files can be examined without alteration or damage.
2. Should the person from whom the computer/hard disk was seized apply under section 488.1(9) of the Criminal Code to make a copy of the seized hard disk, that an CSERS of the Canada Border Services Agency should be requested to carry out the copying process under your control.

Note: It is possible for a Canada Border Services Agency CSERS to carry out the above processes without personally viewing the file or document contents of the seized computer.

The assistance offered and the requests made above are done with an aim to ensuring the integrity of the original seized electronic evidence.

Should you require the assistance of a Canada Border Services Agency Investigator trained in computer search & evidence recovery, please contact [*insert the name of the Investigator*] at [*insert the telephone number of the Investigator*].

Sincerely,
