U.S. Customs & Border Protection
San Juan Field Office
January 23, 2008

Inspection of Portable Hard Drives

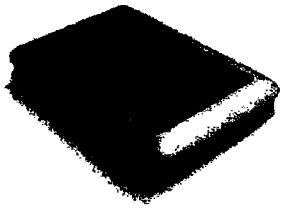
CBP Intelligence Office in its Homeland Security Intelligence Report dated Janaury 23, 2008 reported the apprehension of an F1 visa holder who was in possession of a portable hard drive hidden in his suitcase which contained decapitation videos among others (e.g., child pornography, etc.).

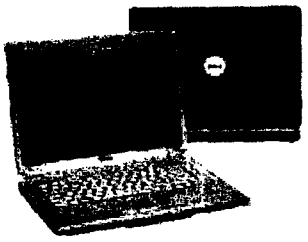
Portable hard drives can carry up to 100 GB of digital music, video, photos, and data files. Some of this handy and compact little drives can even weigh less than one pound making it easy to carry in a briefcase or backpack. These external hard drives allow the users to take a lot of information with them wherever they go.

On July 26, 2007 the HQs disseminated to all ports of entry the interim guidance on examination, copying, and transmittal of documents and electronic media devices as well as the transmittal form.

It is extremely important that all supervisors review this interim guidance once again and ensure it is further discussed with our field officers. In particular with officers who are currently assigned to performing [redacted] inspections.

(b)(2) + (b)(7)(E)





Reference:

HSIR: CBP-027-08

CBP Weekly Muster 2007-11

(b)(2) + (b)(7)(E)

Legal Guidance: Interim Procedures for Border Search/Examination of Documents, Papers, and Electronic Information [redacted]

(b)(2) & (b)(7)(E)

Prepared by:
San Juan Field Office
Operations Branch
(787) 729-6982

Interim Procedures for Border Search/Examination of Documents, Papers, and Electronic Information (b)(2) & (b)(7)(E)

The purpose of this document is to clarify operational guidance with respect to the review and retention of paper documents as well as information in electronic devices (e.g., laptop computers, cell phones, MP3 players) and electronic storage media (e.g., DVDs, CDs, diskettes, memory cards/sticks, thumbnail drives) (collectively, "electronic devices").[1] (b)(2) & (b)(7)(E)
(b)(2) & (b)(7)(E)

CBP's information handling authority under the customs laws is currently reflected in CD 3340-006A, *Procedures for Examining Documents and Papers*. CBP also has broad authority respecting documents under the immigration laws, which has not been fully integrated into CBP policy.

(b)(2) & (b)(7)(E)

(b)(2) & (b)(7)(E) These interim provisions incorporate CBP authority under customs, immigration, and other laws.

1. Initial Review.

Absent individualized suspicion, paper documents and electronic devices may be reviewed in the course of administering customs, immigration, or other laws enforced or administered by CBP.[3]

2. Copying and Transmitting

a. Consistent with existing policy, where technical assistance is necessary to determine the existence of a violation of customs, immigration, or other law enforced or administered by CBP, officers may copy and transmit documents

---

[1] The guidance in this memorandum does not pertain to notes, reports, or other impressions recorded by CBP officers in the course or as the product of a border encounter.

[2] (b)(2) & (b)(7)(E)
p

[3] Note that existing provisions from CD 3340-006A, and the International Mail Operations and Enforcement Handbook, CIS HB 3200-006A, remain in place regarding the opening of sealed letter class mail, including the prohibition against reading correspondence therein. With respect to information other than letter class mail, officers may read correspondence that appears to bear upon a determination under the laws enforced or administered by CBP. In addition, existing guidance from CD 3340-006A remains in place, (b)(2) & (b)(7)(E) regarding attorney-client privileged information; any claim of attorney-client or attorney work product privilege with respect to information encountered in the border context should be coordinated with the appropriate Associate/Assistant Chief Counsel.

and information in electronic devices to an appropriate agency or entity *without individualized suspicion.* This may be the case where translation is required to decipher the contents of a document.

b. Except as provided in the preceding subsection, officers may copy and transmit documents and information from electronic devices only where there is *reasonable suspicion* that (b)(2) & (b)(7)(E) the information may relate to, terrorist activities or other unlawful conduct. Reasonable suspicion is not required if (b)(2) & (b)(7)(E) consents to copying and transmission.

(b)(2) & (b)(7)(E)

3. Retention, Seizure, and Destruction.

a. CBP may retain relevant information in DHS and CBP record systems such as TECS, the immigration A-file system, or related systems, to the extent authorized by law. Nothing in this policy guidance alters existing policies and procedures for retaining documents and information in the immigration A-file system or related systems.

b. Copies of documents or information from electronic devices provided to another agency or entity for the purpose of rendering technical assistance shall be returned to CBP as expeditiously as possible.[4] Where information is returned to CBP and determined to be of no relevance to customs, immigration, or any other laws enforced or administered by CBP, that information will be destroyed.

c. There may be situations where an agency or entity, in furtherance of its respective mission, wishes to retain or disseminate copies of the information provided to it by CBP for technical assistance. Any such retention and/or dissemination will be governed by that agency or entity's existing legal authorities and policies, including concerning periodic reviews of retained materials to evaluate and ensure continued relevancy.

* * *

The above guidance does not alter the authority or ability of officers to seize, disseminate, or retain documents and information in electronic devices (b)(2) & (b)(7)(E) where there is probable cause to believe that such

[4] This period of time, unless otherwise approved by the DFO in consultation with the appropriate Associate/Assistant Chief Counsel, shall be not longer than 15 days from transmittal to the assisting agency, with that time period subject to extensions, in increments not longer than 7 days that are requested and justified by the assisting agency.

documents or information constitute evidence of a crime or are otherwise subject to seizure and forfeiture.

This guidance is intended to augment and clarify paragraphs 6.5.2, 6.5.3, and 6.9.11 of CBP Directive 3340-021B, *Responding to Potential Terrorists Seeking Entry Into the United States* (September 7, 2006). CBP officers and agents, in (b)(2) & (b)(7)(E) and otherwise, must give particular consideration to this guidance in determining how to implement (b)(2) & (b)(7)(E) (b)(2) & (b)(7)(E) from other agencies regarding the collection of information from a given traveler. Field offices are responsible for the development of an appropriate mechanism to ensure the proper tracking of information processed pursuant to this memorandum. No traveler information may be reviewed or retained in contravention of the above provisions, unless approved in advance by the Director, Field Operations in consultation with the appropriate Associate/Assistant Chief Counsel.