Laptop Inspections Legal, Rare, Essential

(08/11/2008) I'd like to address some questions and some misinformation that are circulating with regard to CBP's long-standing policy on searches of electronic media.

First, it's important to note that for more than 200 years, the federal government has been granted the authority to prevent dangerous people and things from entering the United States. Our security measures at the border are rooted in this fundamental fact, and our ability to achieve our border mission would be hampered if we did not apply the same search authorities to electronic media that we have long-applied to physical objects--including documents, photographs, film and other graphic material. Indeed, there are numerous laws that apply to such material at the border including laws regarding intellectual property rights, technical data that can be imported or exported only under state department license and child pornography.

In the 21st century, terrorists and criminals increasingly use laptops and other electronic media to transport illicit materials that were traditionally concealed in bags, containers, notebooks and paper documents. Making full use of our search authorities with respect to items like notebooks and backpacks, while failing to do so with respect to laptops and other devices, would ensure that terrorists and criminals receive less scrutiny at our borders just as their use of technology is becoming more sophisticated.

This result would be ironic given that this same technology actually enables terrorists and criminals to move large amounts of information across the border via laptops and other electronic devices. At the end of the day, we have a responsibility to search items — electronic or otherwise — that are being transported across our borders and that could potentially be used to harm our nation's citizens or that are otherwise contrary to law.

Second, this is not a new policy. We've been searching laptops of those who warrant a closer inspection for years. In fact, we've taken the unprecedented step of posting online a policy that would typically be reserved for internal purposes. This information is not new and has been publicly debated countless times. Indeed, the 9th Circuit Court of Appeals recently confirmed the constitutionality of suspicionless laptop searches at the border.

(U.S. Customs and Border Protection Policy Regarding Border Search of Information (pdf - 161 KB.))
(Circuit Court Ruling)

This brings me to my third point, which is that travelers whose laptops are searched represent a very small number of people. As Secretary Chertoff noted in a recent op-ed, "Of the approximately 400 million travelers who entered the country last year, only a tiny percentage were referred to secondary baggage inspection…[and] of those, only a fraction had electronic devices that may have been checked." (Searches are Legal, Essential)

And finally, to allay any concerns the business community or others may have that their personal or trade information might be put at risk by traveling with their laptops, I urge you to look at our track record. Every day, thousands of commercial entry documents, shipping manifests, container content lists, and detailed pieces of company information are transmitted to CBP so we can effectively process entries and screen cargo shipments bound for the United States. This information is closely guarded and governed by strict privacy procedures. Information from passenger laptops or other electronic devices is treated no differently.

Our Customs and Border Protection officers are trained professionals with a defined mission, and they have neither the time nor the desire to search travelers' personal belongings for any reason other than to ensure compliance with our customs and related laws and to protect the United States. As the policy's provisions make abundantly clear, officers are subject to numerous policy restrictions regarding the retention, sharing, and scrutiny of travelers' documents and information.

I hope this has helped answer some of your questions. One of the lessons 9/11 taught us was that we must adapt to 21st century risks and anticipate rather than react to new threats. Our CBP officers are on the front lines every day ensuring that these lessons are heeded. We trust that travelers understand the need for these sensible security measures.

Jayson Ahern
Deputy Commissioner, U.S. Customs and Border Protection

U.S. Customs and Border Protection

Policy Regarding Border Search of Information

July 16, 2008

This policy provides guidance to U.S Customs and Border Protection (CBP) Officers, Border Patrol Agents, Air and Marine Agents, Internal Affairs Agents, and any other official of CBP authorized to conduct border searches (for purposes of this policy, all such officers and agents are hereinafter referred to as "officers") regarding the border search of information contained in documents and electronic devices. More specifically, this policy sets forth the legal and policy guidelines within which officers may search, review, retain, and share certain information possessed by individuals who are encountered by CBP at the border, functional equivalent of the border, or extended border. This policy governs border search authority only; nothing in this policy limits the authority of CBP to act pursuant to other authorities such as a warrant or a search incident to arrest.

A. Purpose

CBP is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, officers may examine documents, books, pamphlets, and other printed material, as well as computers, disks, hard drives, and other electronic or digital storage devices. These examinations are part of CBP's long-standing practice and are essential to uncovering vital law enforcement information. For example, examinations of documents and electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography, monetary instruments, and information in violation of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

Notwithstanding this law enforcement mission, in the course of every border search, CBP will protect the rights of individuals against unreasonable search and seizure. Each operational office will maintain appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this policy.

B. Review of Information in the Course of Border Search

Border searches must be performed by an officer or otherwise properly authorized officer with border search authority, such as an ICE Special Agent. In the course of a border search, and absent individualized suspicion, officers can review and analyze the information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States, subject to the requirements and limitations provided herein. Nothing in this policy limits the authority of an officer to make written notes or reports or to document impressions relating to a border encounter.

C. Detention and Review in Continuation of Border Search

(1) Detention and Review by Officers. Officers may detain documents and electronic devices, or copies thereof, for a reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location. Except as noted in section D below, if after reviewing the information there is not probable cause to seize it, any copies of the information must be destroyed. All actions surrounding the detention will be documented by the officer and certified by the Supervisor.

(2) Assistance by Other Federal Agencies or Entities.

(a) Translation and Decryption. Officers may encounter information in documents or electronic devices that is in a foreign language and/or encrypted. To assist CBP in determining the meaning of such information, CBP may seek translation and/or decryption assistance from other Federal agencies or entities. Officers may seek such assistance absent individualized suspicion. Requests for translation and decryption assistance shall be documented.

(b) Subject Matter Assistance. Officers may encounter information in documents or electronic devices that is not in a foreign language or encrypted, but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by CBP. With supervisory approval, officers may create and transmit a copy of information to an agency or entity for the purpose of obtaining subject matter assistance when they have reasonable suspicion of activities in violation of the laws enforced by CBP. Requests for subject matter assistance shall be documented.

(c) Original documents and devices should only be transmitted when necessary to render the requested assistance.

(d) Responses and Time for Assistance.

(1) Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include any findings, observations, and conclusions relating to the laws enforced by CBP.

(2) Time for Assistance. Responses from assisting agencies are expected in an expeditious manner so that CBP may complete its border search in a reasonable period of time. Unless otherwise approved by the principal field official such as the Director, Field

Operations or Chief Patrol Agent, responses should be received within fifteen (15) days. This timeframe is to be explained in the request for assistance. If the assisting agency is unable to respond in that period of time, CBP may permit extensions in increments of seven (7) days. For purposes of this provision, ICE is not considered to be a separate agency.

(e) Destruction. Except as noted in section D below, if after reviewing information, probable cause to seize the information does not exist, any copies of the information must be destroyed.

D. Retention and Sharing of Information Found in Border Searches

(1) By CBP.

(a) Retention with Probable Cause. When officers determine there is probable cause of unlawful activity—based on a review of information in documents or electronic devices encountered at the border or on other facts and circumstances—they may seize and retain the originals and/or copies of relevant documents or devices, as authorized by law.

(b) Other Circumstances. Absent probable cause, CBP may only retain documents relating to immigration matters, consistent with the privacy and data protection standards of the system in which such information is retained.

(c) Sharing. Copies of documents or devices, or portions thereof, which are retained in accordance with this section, may be shared by CBP with Federal, state, local, and foreign law enforcement agencies only to the extent consistent with applicable law and policy.

(d) Destruction. Except as noted in this section, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

(2) By Assisting Agencies and Entities.

(a) During Assistance. All documents and devices, whether originals or copies, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to CBP.

(b) Return or Destruction. At the conclusion of the requested assistance, all information must be returned to CBP as expeditiously as possible. In addition, the assisting Federal agency or entity must certify to CBP that all

copies of the information transferred to that agency or entity have been destroyed, or advise CBP in accordance with section 2(c) below.

(i) In the event that any original documents or devices are transmitted, they must not be destroyed; they are to be returned to CBP unless seized based on probable cause by the assisting agency.

(c) Retention with Independent Authority. Copies may be retained by an assisting Federal agency or entity only if and to the extent that it has the independent legal authority to do so—for example, when the information is of national security or intelligence value. In such cases, the retaining agency must advise CBP of its decision to retain information on its own authority.

E. Review and Handling of Certain Types of Information

(1) Business Information. Officers encountering business or commercial information in documents and electronic devices shall treat such information as business confidential information and shall take all reasonable measures to protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may govern or restrict the handling of the information.

(2) Sealed Letter Class Mail. Officers may not read or permit others to read correspondence contained in sealed letter class mail (the international equivalent of First Class) without an appropriate search warrant or consent. Only articles in the postal system are deemed "mail." Letters carried by individuals or private carriers such as DHL, UPS, or Federal Express, for example, are not considered to be mail, even if they are stamped, and thus are subject to a border search as provided in this policy.

(3) Attorney-Client Privileged Material. Occasionally, an individual claims that the attorney-client privilege prevents the search of his or her information at the border. Although legal materials are not necessarily exempt from a border search, they may be subject to special handling procedures.

Correspondence, court documents, and other legal documents may be covered by attorney-client privilege. If an officer suspects that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the officer must seek advice from the Associate/Assistant Chief Counsel or the appropriate U.S. Attorney's office before conducting a search of the document.

(4) Identification Documents. Passports, Seaman's Papers, Airman Certificates, driver's licenses, state identification cards, and similar government identification documents can be copied for legitimate government purposes without any suspicion of illegality.

F. No Private Right Created

This document is an internal policy statement of CBP and does not create any rights, privileges, or benefits for any person or party.