

Office of Public Affairs
U.S. Department of
Homeland Security



**Homeland
Security**

Public Affairs Guidance

BORDER SEARCH POLICY

LAST MODIFIED

Tuesday, September 30, 2008 11:30 a.m. EDT

Background

Secretary Chertoff's interview with Wired:

<http://blog.wired.com/27bstroke6/2008/08/chertoff.html>

Deputy Commissioner Ahern's testimony:

http://www.cbp.gov/xp/cgov/newsroom/congressional_test/laptop_searches.xml

6-30-08 LJ: <http://www.dhs.gov/journal/leadership/2008/06/cbp-laptop-searches.html>

8-5-08 LJ: <http://www.dhs.gov/journal/leadership/2008/08/answering-questions-on-border-laptop.html>

USA Today Op-Ed from Secretary Chertoff, ran 7/16/08

Since the founding of the republic, the federal government has held broad authority to conduct searches at the border to prevent the entry of dangerous people and goods. In the 21st century, the most dangerous contraband is often contained in laptop computers or other electronic devices, not on paper. This includes terrorist materials and despicable images of child pornography.

Laptop searches have proven essential to detecting people and materials that should be blocked from entering the United States. Officers have discovered video clips of improvised explosive devices being detonated, a martyrdom video and other violent jihadist materials. In addition, these searches have uncovered scores of instances of child pornography, including a home movie of children being sexually assaulted.

How often do we search laptops? Of the approximately 400 million travelers who entered the country last year, only a tiny percentage were referred to secondary baggage inspection for a more thorough examination. Of those, only a fraction had electronic devices that may have been checked.

As a practical matter, travelers only go to secondary when there is some level of suspicion. Yet legislation locking in a particular standard for searches would have a dangerous, chilling effect as officers' often split-second assessments are second-guessed.

Are these searches legal? The U.S. Supreme Court has recognized the "right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." And every federal appellate court in the country to address the laptop issue — including the 9th Circuit — has concluded that, at the border, there is no constitutional basis for treating laptops differently than hard copy documents.

We are, of course, mindful of travelers' privacy. No devices are kept permanently unless there is probable cause. Likewise, any U.S. citizen's information that is copied to facilitate a search is retained only if relevant to a lawful purpose such as a criminal or national security investigation, and otherwise is erased. Special privacy procedures govern the handling of commercial and attorney-client information.

We cannot abandon our responsibility to inspect what enters the U.S. just because the information is on an electronic device. To do so would open a dangerous window for terrorists and criminals to exploit our borders in new and unacceptable ways.

Talking Points

- From August 1-13, 2008, CBP processed almost 17 million persons. Of those, around 315,000 (less than 2 percent) were sent for secondary inspection. Only 40 had their laptops even looked at — as minimal a search as a request to turn the laptop on to ensure it isn't filled with contraband. This represents 0.01 percent of all persons sent to secondary.
- The odds in August 2008 of having your laptop searched (not seized -- that would be even more unlikely) are 1 in 421,225. By comparison, the odds of being struck by lightning in a given year are 1 in 400,000 (Source: National Weather Service). You are literally more likely to be struck by lightning than have your laptop searched.
- The tragic events of 9/11 required the federal government to reexamine its law enforcement and counterterrorism efforts to ensure that all legally available means are employed to prevent another attack. Many of these efforts focused on the U.S. border. At the same time, with the creation of the Department of Homeland Security in March 2003, CBP became responsible for immigration functions at the border, in addition to its traditional customs mission.
- Updating our policies reflects an effort to be more transparent. The decision of U.S. Customs and Border Protection to change some of the standards in its old policies reflects the realities of the post-9/11 environment, the agency's expanded mission and legal authorities, and developments in the law, including the Homeland Security Act of 2003. Although certain aspects of the policies have changed, the policies have

always reflected the notion that officers have the constitutional authority to inspect information presented at the border without individualized suspicion.

- CBP Officers are trained to protect information under strict policies that restrict access to sensitive information, including guarding against the inappropriate handling and disclosure of privileged information such as attorney-client communications, or sensitive business information such as trade secrets. If during an examination, a passenger states that his/her items are privileged as a result of attorney-client privilege, then CBP Officer will notify the supervisor of this situation. If the CBP 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 Supervisory CBP Officer will seek advice from the CBP Office of the Chief Counsel or the appropriate United States Attorney's office before conducting a search of the document.
- CBP Officers have the authority and obligation to determine travelers' admissibility to the U.S. In order to determine admissibility, officers ask questions to determine intent of travel. In the course of interviewing travelers, certain questions may be relevant to admissibility determinations that relate to an alien's purpose for entering the United States under visa categories such as R-1 (religious), missionary work under B-1, vocational volunteer work as a B-2, exchange program as a J-1, or seminary study as an F-1.
- Since the founding of the republic, the federal government has held broad authority to conduct searches at the border to prevent the entry of dangerous people and goods. The U.S. Supreme Court has recognized the "right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." And every federal appellate court in the country to address the laptop issue — including the 9th Circuit — has concluded that, at the border, there is no constitutional basis for treating laptops differently than hard copy documents. In the 21st century, the most dangerous contraband is often contained in laptop computers or other electronic devices, not on paper.
- Laptop searches have proven essential to detecting people and materials that should be blocked from entering the United States. Officers have discovered video clips of improvised explosive devices being detonated, a martyrdom video and other violent jihadist materials. In addition, these searches have uncovered scores of instances of child pornography, including a home movie of children being sexually assaulted.
- As a practical matter, travelers only go to secondary when there is some level of suspicion. Yet legislation locking in a particular standard for searches would have a dangerous, chilling effect as officers' often split-second assessments are second-guessed. Of the approximately 400 million travelers who entered the country last year, only a tiny percentage were referred to secondary baggage inspection for a more thorough examination. Of those, only a fraction had electronic devices that may have been checked.

- We are, of course, mindful of travelers' privacy. No devices are kept permanently unless there is probable cause. Likewise, any U.S. citizen's information that is copied to facilitate a search is retained only if relevant to a lawful purpose such as a criminal or national security investigation, and otherwise is erased. Special privacy procedures govern the handling of commercial and attorney-client information. We cannot abandon our responsibility to inspect what enters the U.S. just because the information is on an electronic device. To do so would open a dangerous window for terrorists and criminals to exploit our borders in new and unacceptable ways.

Q&A

Q1. An email sent from CBP's Chief of Passenger Operations in the New York Field Office on July 11, 2007, obtained by the Asian Law Caucus/EFF, indicates interest from other law enforcement agencies in CBP's ability to collect information from travelers. "As we all know, CBP's data collection capabilities have been widely discussed in the law enforcement community and we have been asked by many various agencies to copy and transmit documentation being carried by travelers for legitimate law enforcement reasons," said the writer, whose name was redacted. The writer was seeking from CBP headquarters "clarification on our statutory authority to do that." Can you state whether any clarification has been issued?

A1. Searches at the border searches are done only in furtherance of CBP's law enforcement mission, which includes the administration of numerous laws. CBP Officers are trained in their statutory authorities to perform border searches under well established constitutional and statutory authority, including, but not limited to, 8 USC sec. 1357 and 19 USC sec. 1581, 1582. In performing such searches, CBP may, under authority such as 19 USC sec. 507, and as noted in the July 16, 2008 policy, seek the assistance and expertise of other agencies in understanding merchandise or information that is presented for examination at the border.

Other agencies do not instruct DHS to collect information for them. CBP officers are trained to know under what circumstances sensitive law enforcement information may be shared, with whom, and what the rules are for that information.

In one case, the FBI informed DHS agents that a foreign national allegedly stole proprietary software programs from a U.S. company and attempted to sell the software to the People's Republic of China (PRC). Two of the software programs were both controlled items for export under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR). This suspect traveled from China to the United States to attend a defense conference. ICE agents coordinated with CBP to conduct a border search of the suspect and his belongings when he entered the United States. During the search, CBP officers identified a laptop computer and portable hard drive belonging to him. A preliminary search of the laptop revealed that it contained software belonging to the American company that was a controlled item for export under ITAR. This suspect was sentenced to two years incarceration for violations of 18

USC sec. 1831, the Economic Espionage Act; and 22 USC sec. 2778, the Arms Export Control Act. He also received a \$10,000 fine and 3 years probation.

Q2. There is a memo to the Tucson Field Office about interviewing persons of interest, which from June 2005 onward were being called "suspected terrorists." The memo says that "HQ has advised that they are in the process of creating a national database and suite of targeting tools," using as a "model," the Tucson field office database. What is that national database and suite of targeting tools?

A2. This information is considered law enforcement sensitive information, and we are not at liberty to discuss it publicly.

Q3. The memo also talks about a worksheet/checklist to be used in conjunction with CBP directive 3340-021A (Responding to Potential Terrorists Seeking Entry into the United States). Does that checklist include or cover questions about religion, such as what mosques a person has worshipped in and what the titles of the lectures he has given are?

A3. The checklist is considered law enforcement sensitive information, as is reflected in the redaction of significant portions of the checklist in the ALC-EFF FOIA production.

Q4. Have you ever broadly disclosed the 1986 or 2000 border policies on examination of documents, and if so, when, and to whom?

A4. As a historical matter, the referenced policies are considered public, and thus would have been disclosed routinely in response to requests.

Q5. Are border personnel either instructed to, or permitted to ask travelers questions such as: What mosques they have prayed in, what charities they have donated to, what lectures they have given, what the titles of the lectures are? Under what authorities are they allowed to ask those questions? Are such questions within the bounds of the First Amendment? Was there any change in policy in the 2005 - 2006 time frame that permitted or instructed border personnel to ask such questions of travelers pulled aside for secondary screening?

A5. CBP Officers have the authority and obligation to determine the admissibility of non-U.S. citizens into the United States. In order to determine admissibility, officers ask questions to determine intent of travel. In the course of interviewing non-U.S. citizens, certain questions may be relevant to admissibility determinations that relate to an alien's purpose for entering the United States under visa categories such as R-1 (religious), missionary work under category B-1, vocational volunteer work under category B-2, exchange program under category J-1, or seminary study under category F-1.

In addition to authority to question regarding the admissibility of merchandise under the customs laws and myriad other federal laws that are enforced at the border, 8 USC 1357(b) provides CBP with authority, in pertinent part and that is not limited to aliens,

“to administer oaths and to take and consider evidence concerning the privilege of any person to enter, reenter, pass through, or reside in the United States.”

Q6. U.S. Customs Service policies in 1986 and 2000 specified that probable cause was required to seize and to copy documents. The July 2008 policy specified that documents may be detained for a reasonable amount of time, and copies made. No standard was specified. Also, the 1986 and 2000 policies specified that reasonable suspicion was required to read and continue to detain documents. The July 2008 policy specified that review could take place absent individualized suspicion. What is the justification for relaxing the legal standards in both instances?

A6. The 1986 and 2000 U.S. Customs Service policies were issued prior to the 2002 Homeland Security Act (“HSA”), 6 U.S.C. secs. 101-557. The Homeland Security Act was a response by Congress and the Administration to the tragic events of 9/11, which required the federal government to reexamine its law enforcement and counterterrorism efforts to ensure that all legally available means are used to prevent another attack. Many of these efforts focused on increasing security at the U.S. border, particularly with regard to admissibility of non-U.S. citizens. With the creation of the Department of Homeland Security in March 2003, CBP became responsible for immigration functions at the border, in addition to its traditional customs mission. CBP’s decision to change its old policies reflects the realities of the post-9/11 environment, the agency’s expanded mission and legal authorities, and developments in the law, including the Homeland Security Act of 2002. Although certain aspects of the policies have changed, the policies have always reflected the notion that officers have the constitutional authority to inspect information presented at the border without individualized suspicion.

Q7. In 1988, in *Heidy v. U.S. Customs Service*, the U.S. District Court, Central District, in California enjoined the U.S. Customs Service from sharing information obtained at the border with other federal agencies unless those agencies abided by Customs’ own restrictions. How would you square that with the July 2008 policy, which allows Customs to share data with other federal agencies, which may retain copies of the data to the extent that they have independent legal authority to do so?

A7. The injunction in *Heidy* only covered materials, or copies thereof, detained for a determination of seizability under 19 U.S.C. sec. 1305 (relating to seditious materials). Since the issuance of that decision, CBP amended its directive governing section 1305, and that directive remains in place. As noted above, particularly after the enactment of the Homeland Security Act, CBP is responsible for enforcing, and ensuring appropriate and lawful information sharing in connection with, numerous other laws at the border.

Q8. The rationale of the *Heidy* decision appears to be that if CBP seeks the assistance of other agencies in determining whether there is a violation of a law enforced by CBP, the other agencies’ rights to the materials should be subject to the same rules and restrictions as CBP. But that is not the case in the current policy. Why not? (Side point: I know you said that CBP amended its directive governing

Section 1305 on seditious materials, but the July 2008 policy makes no mention of Section 1305).

A8. The CBP directive governing 19 USC 1305 relating to sedition remains in place and was not superseded by the policy of July 16, 2008.

Q9. Can you walk me through the process of data acquisition and retention? Who typically initiates those requests for data? Does the Customs officer first notify the FBI? Are there MOUs between the FBI and Customs? IRS and Customs?

If, during an examination, a CBP Officer identifies a need to detain a document or electronic device for a reason listed in the July 16, 2008 policy, then the CBP Officer performing the examination must request a Supervisory CBP Officer's approval. The Supervisory CBP Officer will then determine if there is a need for the detention and whether this detention is consistent with agency policy. If the Supervisory CBP Officer approves of the detention, then the Supervisory CBP Officer will decide on whether the item itself will be detained or if an electronic copy of the media will need to be made. If the item itself is detained, then the passenger will receive a receipt for this detained item. If the decision is to make an electronic copy, then CBP will usually request assistance from Immigration and Customs Enforcement for the copying of this media. These requests typically come from CBP Officers as a result of the performance of their examination. Unless there is a particular reason for involving the FBI or IRS, those agencies would not typically be notified of a detention of information. We are not aware of MOUs with the FBI or IRS that address this subject.

Q10. A large volume of data can be retrieved by copying the contents of laptops and cell phones, including e-mail and IM chats. Are there any internal restrictions on reading email? Chat sessions? Recovering passwords? Recovering deleted files? Medical records? Associational activities – such as what groups you're a member. How do you know as a practical matter whether the person whose data has been acquired is a journalist? A lawyer? A priest? That a document is privileged? How do you make that determination? How do the agencies that you share the info with make that determination?

A10. CBP Officers are trained to protect information under strict policies that restrict access to, and disclosure of, sensitive information, including guarding against the inappropriate handling and disclosure of privileged information such as attorney-client communications, or sensitive business information such as trade secrets. Any employee who violates CBP policy or federal law may be subject to sanctions or other discipline. If during an examination, a passenger states that his/her items are privileged as a result of attorney-client privilege, then CBP Officer will notify his or her Supervisor of this situation. If the CBP 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 Supervisory CBP Officer will seek advice from the CBP Office of the Chief Counsel or the appropriate United States Attorney's office before conducting a search of the document.

Q11. The July 2007 interim Border Search policy states that it was intended to augment and clarify portions of the Directive on Responding to Potential Terrorists Seeking Entry into the United States. How so? Does that directive have any language on questioning individuals about religion or politics? Is there any specific policy constraining Customs officials from questioning travelers about religion or politics?

A11. The July 2007 interim policy augmented DHS directives governing examinations of information in the possession of a traveler, saying that those examinations be performed in accordance with existing policy and any successor directives. That directive does not instruct officers regarding the questioning of individuals about religion or politics. To the extent that any such directives may exist that relate to questioning on religion or politics, they would have been provided in response to the referenced FOIA request of the Asian Law Caucus and the Electronic Frontier Foundation – which includes agency guidance on issues such as processing travelers seeking asylum from persecution for religious or political reasons, and the processing of travelers on a religious worker R visa. CBP Officers have the authority and obligation to determine travelers' admissibility to the U.S. In order to determine admissibility, officers must ask questions to determine intent of travel. In the course of interviewing travelers, certain questions may be relevant to admissibility determinations that relate to an alien's purpose for entering the United States under visa categories such as R-1 (religious), missionary work under category B-1, vocational volunteer work as a category B-2, exchange program as a category J-1, or seminary study as a category F-1.