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

Homeland Security

Public Affairs Guidance

BORDER SEARCH POLICY

LAST MODIFIED
Thursday, October 23, 2008 8:20 p.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 there is probable cause 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

- Searches of laptops and other electronic media during secondary inspection are a targeted tool that CBP uses in limited circumstances to ensure that dangerous people and dangerous goods do not enter our country.

- Laptop and electronic media searches are only applied to a small percentage of passengers in secondary inspection, the vast majority of whom are referred to secondary because CBP has a specific reason to subject them to greater scrutiny.

- CBP's policy applies only to international travelers seeking to enter or depart the United States at a Port of Entry, and to persons apprehended at the border attempting to illegally enter the country between the ports of entry.

- For August, 2008, CBP processed more than 38 million persons and vehicles. Of those, 748,500 (less than 2 percent) were sent for secondary inspection. Only 139 of those referred to secondary had their laptops even looked at – in some cases, with the inspection consisting only of a request to turn the laptop on to ensure it isn't filled with contraband.

- 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. With the creation of the Department of

Homeland Security in March 2003, CBP assumed an expanded law enforcement mission, becoming responsible for immigration functions at the border, in addition to its traditional customs mission.

- Updating and posting our policies reflects an effort to be more transparent. The decision of U.S. Customs and Border Protection to consolidate and update some of the standards in prior 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, officers have always had 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.

- 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, including instructions on how to create cell phone detonators for bombs. In addition, these searches have uncovered scores of instances of child pornography, including a home movie of children being sexually assaulted. In the 21st century, the most dangerous contraband is often contained in laptop computers or other electronic devices, not on paper. And the fact that a single laptop hard drive can contain volumes of information gives CBP a greater need, not a lesser need, to examine it to know what is passing across our sovereign borders.

- As a practical matter, travelers almost always receive a full secondary inspection only when there is some level of suspicion. Legislation locking in a particular standard for searches would have a dangerous, chilling effect as officers' often split-second assessments are second-guessed. Moreover, there are special situations where it may be necessary for officers to search based on general intelligence rather than suspicion as to a particular person (e.g., consider that following scenario: information is received by DHS that a male between 20 and 40 years old will be entering the U.S. from the UK during a specific week and the person will be carrying a laptop containing instructions for a terrorist attack in the U.S. Based on this information, it would be entirely reasonable for CBP to perform laptop searches on all such males arriving in the U.S. from the UK that week.) However, as a practical matter 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, again almost always when there was at least some suspicion that triggered the further search of their electronic device.

- 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 by DHS only if there is probable cause, 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.

- 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." "United States v. Ramsey, 431 U.S. 606, 619 (1977). 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 information in electronic devices differently than hard copy documents.

    - Circuit Judge Diarmuid O'Scannlain wrote in the panel's April 21 decision in the case of **U.S. v Arnold, filed April 21 2008 by the United States Court of Appeals, Ninth Circuit,** that "Courts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment," O'Scannlain wrote. "We are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."

    - The opinion in **U.S. v. Ickes, filed January 4 2005 by the United States Court of Appeals, Fourth Circuit,** stated "The border search doctrine is not a recent development in the law. The "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself. "United States v. Ramsey, 431 U.S. 606, 619 (1977). In fact, the same Congress which proposed the Fourth Amendment to state legislatures also enacted the first far-reaching customs statute in 1790. Id. at 616. Thus, since the birth of our country, customs officials have wielded broad authority to search the belongings of would-be entrants without obtaining a warrant and without establishing probable cause."
      Note: The quote in the second half is from the ruling in the Ickes case but references the early case of Ramsey as precedent.

- Case examples of terrorism-related laptop searches (heavily redacted):

  - In 2006, a male passenger traveling on an F-1 student visa arrived at Minneapolis St. Paul Airport from Amsterdam. An examination of his baggage and laptop computer revealed various items of interest, to include:

    - Numerous video clips of Improvised Explosive Devices (IEDs) being exploded against soldiers and vehicles.
    - Instructions for making explosive devices in Arabic.
    - A file showing the passenger reading his will and included pictures of various high level Al-Qaida officials.

    When asked about these files, the passenger refused to answer further questions. The Department of State revoked the subject's visa subsequent to his arrival. Based on this and further derogatory information uncovered by computer forensics, the passenger was refused admission and processed under expedited removal.

  - In 2007, a male passenger arrived at the San Francisco International Airport seeking admission as a U.S. lawful permanent resident. During CBP's inspection of the passenger's laptop computer, CBP officers discovered several items of significance. These items included:

    - A photo of a Canadian passport with an outline of its security features and a fraudulent invitation letter for a cruise ship company.
    - A photo of an electronic circuit with a timing device with numerous wires attached to it.
    - Two files containing martyrdom videos of Palestinian suicide bomber talking about blowing themselves up.

    The laptop was detained for further analysis which aided in the issuance of a Notice to Appear in front of an Immigration Judge. The evidence uncovered during the inspection by CBP was an essential factor for the case. The final disposition of this case favored the Government as the Immigration Judge ruled that the passenger was inadmissible under terrorist related charges under the Immigration and Naturalization Act.

QUESTIONS & ANSWERS

EXTERNAL Q&A

SEARCHES

Why are electronic devices searched at border crossings?

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. 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.

For example, a U.S. citizen was recently arrested for possession of child pornography. The man arrived on a flight from St. Maarten and was a lookout for prior criminal history of child molestation. CBP notified Immigration and Customs Enforcement (ICE) who interviewed him. During questioning, he admitted to having a "work" laptop with him. CBP and ICE asked what was stored on the laptop and he responded "things his friends sent to him". The ICE agent asked him for permission to locate files and folders on the desktop – he agreed. During this search, agents discovered a large cache of pornographic pictures. The man then admitted child porn was saved on the laptop computer. CBP seized the laptop computer and CBP and ICE escorted the man to the local correctional facility.

To which travelers does CBP's policy apply?

CBP's policy applies only to those international travelers at the border who have been referred for secondary inspection, and to persons apprehended at the border attempting to illegally enter the country between ports of entry. Furthermore, the searches are only applied to a small percentage of these passengers, the vast majority of whom are referred to secondary because CBP has a specific reason to subject them to greater scrutiny. The policy does not apply to domestic travelers. Searches of laptops and other electronic media during secondary inspection are a targeted tool that CBP uses in limited circumstances to ensure that dangerous people and dangerous goods do not enter our country.

Who is responsible for conducting these searches – CBP, TSA, other law enforcement officials?

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 materials, 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 have proven essential to detecting people and materials that should be blocked from entering the United States. ICE special agents, who share responsibility with CBP to enforce the customs and immigration laws, also have authority to conduct these border searches.

What percentage of travelers have devices that are searched during border crossing inspections?

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. For example, from Aug 1 – Sep 15, 2008 over 52 million people entered the U.S. ports, but there were only 175 laptop searches.

- In August 2008, CBP encountered more than 38 million travelers at U.S. ports of entry. Of these more than 38 million travelers, approximately 748,500 travelers participated in secondary inspection, but only 139 individuals were subject to a laptop inspection. Therefore, during this period, approximately 0.019 percent of all travelers referred to secondary inspection were subject to a laptop inspection.

- In the first two weeks of September 2008, 14,784,638 primary inspections were conducted; two percent of which underwent secondary inspection. Of those, only 36 documented laptops were searched, meaning that 0.012% of all secondary exams involved searching a laptop computer.

What are the odds that my laptop, or other electronic device, will be searched?

The number of travelers who had a laptop that was searched by CBP officers in the first two weeks of September 2008 was roughly 1 in 410,000. By comparison, the odds of being struck by lightning in a given year are 1 in 400,000 (Source: National Weather Service).

What kind of information are CBP officers looking for when they conduct a laptop search?

In the 21st century, the most dangerous contraband is often contained in laptop computers or other electronic devices. Laptop searches have proven essential to detecting people and materials that should be blocked from entering the United States.

- Case examples of terrorism-related laptop searches (heavily redacted):

- In 2006, a male passenger traveling on an F-1 student visa arrived at Minneapolis St. Paul Airport from Amsterdam. An examination of his baggage and laptop computer revealed various items of interest, to include:

  - Numerous video clips of Improvised Explosive Devices (IEDs) being exploded against soldiers and vehicles.
  - Instructions for making explosive devices in Arabic.
  - A file showing the passenger reading his will and included pictures of various high level Al-Qaida officials.

  When asked about these files, the passenger refused to answer further questions. The Department of State revoked the subject's visa subsequent to his arrival. Based on this and further derogatory information uncovered by computer forensics, the passenger was refused admission and processed under expedited removal.

- In 2007, a male passenger arrived at the San Francisco International Airport seeking admission as a U.S. lawful permanent resident. During CBP's inspection of the passenger's laptop computer, CBP officers discovered several items of significance. These items included:

  - A photo of a Canadian passport with an outline of its security features and a fraudulent invitation letter for a cruise ship company.
  - A photo of an electronic circuit with a timing device with numerous wires attached to it.
  - Two files containing martyrdom videos of Palestinian suicide bomber talking about blowing themselves up.

  The laptop was detained for further analysis which aided in the issuance of a Notice to Appear in front of an Immigration Judge. The evidence uncovered during the inspection by CBP was an essential factor for the case. The final disposition of this case favored the Government as the Immigration Judge ruled that the passenger was inadmissible under terrorist related charges under the Immigration and Naturalization Act.

When did the policy for border search of information contained in documents and electronic devices change and why?

On July 16, 2008, CBP, in coordination with DHS, issued a comprehensive CBP policy, consolidating and updating customs and immigration policies and practices, to address the border search of information contained in documents and electronic devices.

Updating and posting 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, CBP officers have always held the constitutional authority to inspect information presented at the border without individualized suspicion.

The updated policy is available to the public via the CBP website at http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf.

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 absent individualized suspicion.

- Circuit Judge Diarmuid O'Scannlain wrote in the panel's April 21 decision in the case of **U.S. v Arnold, filed April 21 2008 by the United States Court of Appeals, Ninth Circuit,** that "Courts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment," O'Scannlain wrote. "We are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."

- The opinion in **U.S. v. Ickes, filed January 4 2005 by the United States Court of Appeals, Fourth Circuit** stated "The border search doctrine is not a recent development in the law. The "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself. "United States v. Ramsey, 431 U.S. 606, 619 (1977). In fact, the same Congress which proposed the Fourth Amendment to state legislatures also enacted the first far-reaching customs statute in 1790. Id. at 616. Thus, since the birth of our country, customs officials have wielded broad authority to search the belongings of would-be entrants without obtaining a warrant and without establishing probable cause."

What about my personal rights to privacy?

In the course of every border search, CBP will protect the rights of individuals against unreasonable search and seizure.

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 by DHS only if there is probable cause and otherwise is erased. Special privacy procedures govern the handling of commercial and attorney-client information.

Professionally, I handle sensitive information and carry such information on my laptop when I travel. What protections are in place to guarantee that an officer conducting an inspection will not use that information? What about attorney-client privileged information?

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 the 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.

What is the difference between a search, detention, and a seizure/retention?

Search: CBP officers may examine documents, books, pamphlets, and other printed materials, as well as computers, disks, hard drives and other electronic or digital storage devices.

Detention: Officers may detain documents and electronic devices, or copies as appropriate, for a reasonable period of time to perform a thorough border search. If, after reviewing the information, there is not probable cause to seize it, any copies of the information will be destroyed.

Seizure/Retention: When officers determine that 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.

SEIZURES

Why would CBP seize a laptop?

There are various reasons why a CBP Officer would seize a laptop as authorized by federal law. Here are the most common reasons:

1. There is probable cause to believe that a laptop contains contraband such as child pornography images,
2. There is probable cause to believe that the laptop contains information that is evidence of a crime (for example, terrorist plans).

3. There is probable cause to believe that the laptop itself was used in connection with a crime (for example, it belongs to a person arrested for drug smuggling and there is reason to believe that the laptop was used to facilitate the smuggling scheme).

4. There is probable cause to believe that the laptop was acquired abroad and was not declared.

Do a significant number of border crossing inspections result in the seizure of a laptop?

From October, 2006 to August 2008, CBP seized 101 laptops at inbound inspections conducted at airports.

By comparison, Transportation Security Administration (TSA) statistics show that nationally, about 75 laptops are reported lost or missing at our nation's airports each month. More than 2 million passengers go through TSA checkpoints each day. So in the same period of time, TSA would estimate that about 1,725 laptops would have been reported or lost or stolen — more than seventeen times as many as CBP seized.

How many laptop seizures are non-commercial?

There were 65 non-commercial laptop seizures in FY 2008. This term non-commercial denotes a particular laptop seized from an individual traveler. On occasion, CBP also seizes commercial shipments of new laptops for various trade violations, which are considered commercial seizures, which has little to do with this issue.
A majority of these laptops were seized incidentally to arrest or seizure of narcotics and prior system lookouts for various reasons such as child pornography.

If my laptop has been seized, when and how will I get it back?

To be very clear, if a laptop is *detained* for further examination – as opposed to seized on probable cause – CBO issues a "6051-S receipt" to the owner. This receipt includes a CBP address and a phone number which the individual may call for updates on the status of their electronic device. If a laptop is seized as evidence and/or for forfeiture CBP issues a seizure notice to the person. That notice explains the procedures and regulations that the person may follow to contest the seizure and/or forfeiture of the laptop.

INTERNAL Q&A

What type of outreach to Congress has been conducted on these specific issues?

CBP and U.S. Immigration and Customs Enforcement (ICE) have responded to numerous Congressional inquiries for information on searches of electronic devices and have participated in Congressional briefings on this issue. These briefings addressed the

border search examination process and authority with regard to searches of information contained in documents, laptops, and other electronic devices.

What were the CBP statistics and measurement procedures prior to August, 2008?

Prior to August 2008, CBP Officers recorded any noteworthy media and laptop searches in the Inspection Operations Incident Log (IOIL) reporting. To gather data prior to August 2008, analysts used a text query to identify documented electronic media searches. These records were codified using codes developed on July 31, 2008. Laptop seizure information was tracked by an analysis of seized property codes in Seized Asset and Case Tracking System (SEACATS).

Since August 2008, Planning, Program Analysis and Evaluation CBP has tracked nationwide searches directly via the IOIL platform using the newly established/mandated codes.

CBP is continuing to work to improve data retrial in this important area.

How do ports track information/activities related to border searches?

CBP Muster 2008-09, which was distributed to the ports on Aug. 27, 2008, provided new reporting codes for the ports to use at primary and secondary inspection in order to facilitate the tracking of activities related to the border search of information.

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?

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 1357 and 19 USC 1581, 1582. In performing such searches, CBP may, under authority such as 19 USC 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.

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?

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

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?

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.

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

As a historical matter, the referenced policies are considered public, and thus would have been disclosed routinely in response to requests. To our knowledge, they were routinely made available to the public, including pursuant to FOIA requests.

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?

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.

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. [There is an obligation to share terrorism information with certain agencies but as that subject concerns sensitive matters it cannot be discussed].

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?

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.