GC CONFIRMATION ISSUE: Border Search of Laptop Computers
(CBP-OCC/(b)(6); (b)(7)(C))

Background: On April 21, 2008, the United States Court of Appeals for the Ninth Circuit held, "that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." This decision is significant because it upholds the ability of CBP to search electronic devices in one of the largest judicial circuits (the Ninth Circuit covers the entire western portion of the nation, and some of the busiest CBP POEs). The decision also represents the second court of appeals victory for CBP on this issue, as the Fourth Circuit previously upheld the suspicionless border search of a computer and disks found in a vehicle entering the United States from Canada. See U.S. v. Ickes, 393 F.3d 501 (4th Cir. 2005).

In 2005, CBP officers discovered child pornography contained in the defendant's laptop computer during a border search at Los Angeles International Airport. Criminal charges were filed against defendant Michael Arnold. The defense attorney moved to suppress evidence before trial, claiming that CBP needed reasonable suspicion to conduct a border search of electronic files on the laptop computer. The trial court granted defendant's motion and suppressed the evidence, holding that border searches of computers are unconstitutional unless supported by reasonable suspicion, and finding that the facts adduced during the evidentiary hearing did not amount to reasonable suspicion. At oral argument, the government argued that suspicion-less border searches of property are authorized by long-standing precedent and justified by the government's paramount security interest at the border. Further, there are no constitutionally significant differences between laptop computers and other containers for purposes of border search authority. Appellee argued that a search of files on a laptop computer was akin to a personal search.[1]

Question What is your position on border search of electronic media? Is the information stored in electronic media distinguishable from other storage devices that are subject to border search? Absent reasonable suspicion, why would it be appropriate to search files contained in electronic media at the border?

---

[1] The Ninth Circuit sitting en banc recently heard argument in U.S. v. Seljan, a case involving an analogous issue: whether CBP officers must have reasonable suspicion to read what appears to be a personal letter carried by a private express company. In Seljan, CBP officers opened a FedEx package being shipped to the Philippines and read a letter that aroused suspicions that Seljan may have been committing child pornography offenses. Subsequently, CBP officers searched similar shipments by Seljan, and ICE opened an investigation into the matter. This led to Seljan's arrest on child pornography offenses. Seljan was ultimately convicted of these charges and both the trial court and the Ninth Circuit panel ruled against his arguments that CBP officers were required to have reasonable suspicion to read his letter.

Because this is an en banc case, we do not expect a decision until late this year. We are optimistic about winning the case. It is important to note that this case does not involve the search or reading of mail, but rather items being shipped out of the U.S. by a private company. CBP has regulations that apply to mail carrying correspondence, and those rules require CBP officers to have probable cause or consent before reading personal correspondence in the mail. These regulations are not based on the Constitution, but are self-imposed. CBP has always treated papers, film, etc., carried across the border in any manner other than by sealed letter class mail, as merchandise that is subject to border search.

Talking Points:

- Border search of electronic media is constitutionally permissible. Customs officials have longstanding authority under the Fourth Amendment to conduct suspicion-less searches of personal property at the international border. This broad search authority stems directly from the government's paramount interest in protecting the security and integrity of its borders. Further, travelers crossing the border have a substantially diminished expectation of privacy in their personal belongings.

- The Ninth Circuit's decision in U.S. v. Arnold follows the existing case law in other circuits. Courts within the Fourth Circuit (U.S. v. Ickes, 393 F.3d 401 (4th Cir. 2005)), Second Circuit (U.S. v. Irving, 432 F.3d 401 (2nd Cir. 2005)), and Fifth Circuit (U.S. v. Roberts, 274 F.3d 1007 (5th Cir. 2001)) have upheld border searches of electronic media without requiring reasonable suspicion.

- Computers and other electronic media storage devices are neither conceptually nor constitutionally different than other closed storage containers subject to suspicion-less border searches. Personal belongings and effects that are stored in purses, suitcases and briefcases are equally private material, which are justifiably subject to suspicion-less searches at the border under longstanding statutory authority and Supreme Court precedent.

- Suspicion-less searches of computers and other electronic media are justified by the government's paramount interest in border security and are essential to ensure national security, health and public welfare. The border is unique; border searches are performed for self-protection, to gain revenue and to identify items that are being introduced into the country. Accordingly, broad search authority is necessary to further the government's interest in protecting its territorial integrity.

ANTICIPATED QUESTIONS:
SEARCHES

Why are electronic devices searched at border crossings?

- At the border (or its functional equivalent), CBP and ICE have broad authority to conduct searches of persons and things upon their entry into or exit out of the country without first obtaining a warrant and without suspicion. This authority stems from a long-standing and well recognized exception to the Fourth Amendment that is premised on the government's interest in protecting its citizens from the entry of persons and items harmful to U.S. interests. Repeatedly, the Supreme Court has recognized that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[1]

- There are numerous statutory provisions reflecting the authority of ICE and CBP to conduct suspicionless border searches in connection with the inspection of persons, merchandise, baggage, conveyances, and containers, including laptops and other electronic devices, entering the United States.

- In general, CBP and ICE do not distinguish between the search of documents and electronic devices and the search of any other items crossing our borders. DHS along with some federal courts, including the U.S. Court of Appeals for the Ninth Circuit, have concluded that searching documents, including those in electronic form, is well within the broad border search exception exercised by CBP and ICE and have generally endorsed the view that laptop computers or other electronic devices are neither conceptually nor constitutionally different from other closed containers subject to suspicionless searches at the border.

- The exercise of this plenary authority has been a critical component to ensuring national security at U.S. borders. To impose a different inspectional standard for any particular class of merchandise would unnecessarily undermine homeland security.

- With changes in technology over the last several decades, the ability to easily and economically carry vast amounts of information in electronic form has risen dramatically. The advent of compact, large capacity, and inexpensive electronic devices and media, such as laptop computers, thumb drives, compact disks (CD), digital versatile disks (DVD), cell phones, subscriber identity module (SIM) cards, digital cameras, and other devices capable of storing information (hereinafter "electronic media") has encouraged many people to carry very sensitive personal information with them at all times. When these devices and media are carried by a traveler crossing the U.S. border, they and all other belongings are subject to search at the discretion of DHS to ensure the execution

[1] United States v. Ramsey, 431 U.S. 606, 616 (1977).

and enforcement of Federal immigration and customs laws. In particular, CBP and ICE, law enforcement agencies within DHS, conduct border searches of such electronic media as part of their mission to protect the Nation's borders.

- The methods and trends of criminals attempting to bring illicit materials through U.S. borders have changed with technology. The use of electronic media capable of storing information relating to criminal activities has been established as the latest method for smuggling these materials. As the world of information technology evolves, the techniques used by law enforcement agencies such as CBP and ICE must also evolve to identify, investigate, and prosecute individuals using new technologies in the perpetration of crimes. Failure to do so would create a dangerous loophole for criminals seeking to import or export illicit materials, just as their use of technology is becoming more sophisticated.

To which travelers do the CBP and ICE policies apply?

As with all border searches, all international travelers, both inbound and outbound, are subject to search. However, only a small percentage of travelers have been subject to these types of searches and, historically, CBP and/or ICE generally has a reason for subjecting the traveler to greater scrutiny. Searches of laptops and other electronic media are a targeted tool that CBP and ICE use in limited circumstances to ensure that merchandise contrary to law does not cross U.S. borders and that inadmissible persons are not allowed to enter.

Who is responsible for conducting these searches?

As CBP and ICE are responsible for ensuring compliance with customs, immigration and other federal laws at the border, only CBP Officers and ICE Special Agents (and certain USCG officers acting as "customs officers") are legally permitted to conduct border searches

What are you doing to address the concerns that have been made by Congress about these types of searches?

The DHS Privacy Office (PRIV) is conducting a Privacy Impact Assessment (PIA) of current DHS practices involving searches of laptops and other electronic devices at the border. The PIA is being done with substantial contribution and cooperation by CBP and ICE and will provide an element of transparency for Congress and the public on Departmental practices and protections for protecting privacy. I have also asked CBP, ICE, Policy, PRIV and the Office for Civil Rights and Civil Liberties (CRCL) to look at mechanisms to better inform travelers of our policy, procedures and their rights with regard to the search of electronic devices at the border. In response, CBP is also working on a notice to be provided for individuals whose devices are detained by CBP for further investigation so that they will understand the procedure, their rights, how they will be able to retrieve their property and who they can contact if they have questions. DHS will continue to address concerns of members of Congress and ensure that we are as transparent as possible with respect to the search of electronic devices at the border.

Will a Civil Liberties Impact Assessment be conducted?

CRCL has the discretion to conduct a Civil Liberties Impact Assessment on border searches of electronic devices if one is deemed necessary.

We have heard reports that people from certain parts of the world, of Arab ethnicity or of the Muslim faith are disproportionately selected for examination of electronic devices. Is this true?

CBP and ICE do not profile on the basis of race, ethnicity or religion. Our border searches are conducted using far more sophisticated criteria than broad characterizations based on immutable characteristics. Statistically, by far, the United States accounts for the largest nationality grouping of those selected for electronic examination. Individuals can be selected to have their electronic devices examined based on a number of factors that range from specific law enforcement and counter-terrorism information to the skill and abilities of officers to question individuals seeking to bring these devices into the country.

Does DHS make an electronic copy of electronic device that are searched?

Sometimes. CBP or ICE may detain the traveler's original electronic device, or a copy of it, for a reasonable period of time to perform a thorough border search. The continuing border search may take place on-site or at an off-site location (for example, an ICE forensics laboratory). If after reviewing the information – whether the original or copies - there is not probable cause to seize it, any original items will be returned or copies will be destroyed. All actions surrounding the detention are documented by the officer and certified by the Supervisor.

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, CBP or ICE may seize and retain the originals and/or copies of relevant documents or devices, as authorized by law.

Other Circumstances
Absent probable cause, CBP or ICE may only retain documents relating to immigration matters as authorized by law and as consistent with the privacy and data protection standards of the system in which such information is retained.

Destruction
Except as noted in above, if after reviewing information, there is no probable cause to seize the information, CBP and/or ICE will destroy all copies of the information.

Are these copies shared with other agencies?

Sometimes. There are two points at which CBP and/or ICE may share information with other agencies. The first is through a demand for assistance: in conducting a border search, CBP or ICE may require assistance in translating or decrypting the information, so as to complete its search. In addition, ICE may require the assistance of a particular agency with subject matter expertise in order to complete its search. The second time is once CBP or ICE has established probable cause and has seized the information (for criminal purposes) or retained the information (for immigration purposes). Any such sharing is in compliance with applicable SORNs, policies, and laws.

Can other agencies retain a copy of these materials?
Sometimes. Information shared through the two scenarios above may be retained by a Federal agency 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 or ICE of its decision to retain information on its own authority.

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

0.023% - meaning out of every 204,552 persons entering the U.S.,
CBP performs about 1 laptop computer search.

Between October 1, 2008 and April 21, 2009 (FY 2009), CBP Officers encountered more than 134.8 million passengers. Of these, 2.9 million were sent for further secondary screening and inspection (2.2%). Of all passengers that underwent secondary inspection, 659 had an examination that involved a laptop computer. This means that 0.023% of all secondary inspections performed by CBP Officers actually included a laptop computer. Overall, thus far in FY 2009 the odds of a traveler having a search of their laptop computer performed are approximately 1 in 204,552.

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 August 2008 was roughly 1 in 421,000. 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 is CBP or ICE looking for when they conduct a laptop search?

In the 21st century, merchandise contrary to law or evidence of a crime, including that related to terrorism and child exploitation, is often contained in laptop computers or other electronic devices. Laptop searches have proven essential to detecting such information and persons prior to their entry into the United States. The following are case examples of laptop searches resulting in the discovery of terrorism-related information:

- In September, 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 February, 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, which led to expert testimony identifying the passenger as an attractive target for Hamas recruitment, was an essential factor for the case. 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 and ICE, in coordination with DHS, issued separate policies on searching documents and electronic devices at the border. These policies consolidated and updated previous customs and immigration policies and practices and established guidance for detention, seizure, sharing, retention, and destruction of information.

Updating and posting our policies reflects an effort to be more transparent. The decision of CBP and ICE to publish their revised policies reflects the realities of the post-9/11

environment, the agencies' expanded mission and legal authorities, and developments in the law. Although certain aspects of the policies have changed, CBP Officers and ICE Special Agents have always held the constitutional authority to inspect information presented at the border without a warrant or individualized suspicion.

The updated CBP 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. The ICE policy is available to the public through the FOIA process and has been made available during congressional briefings.

I have also been informed that contemporaneous with the issuance of the July 16, 2008, policy, and thereafter, DHS, CBP, and ICE officials under the previous Administration conducted numerous briefings for Congressional staff on the July 16, 2008, policy.

Are these searches legal?

The Supreme Court has recognized the "right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." Every federal appellate court in the country to address the laptop issue — including the 9th and 4th Circuits — have concluded that, at the border, there is no constitutional basis for treating laptops differently than hard copy documents and that such searches may be conducted 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 for the 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." The opinion further explained that, "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."

- In ***U.S. v. Ickes*, filed January 4 2005, by the United States Court of Appeals for the Fourth Circuit**, the court 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. ... In fact, the same Congress which proposed the Fourth Amendment to state legislatures also enacted the first far-reaching customs statute in 1790. 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." *Citing United States v. Ramsey*, 431 U.S. 606, 619 (1977).

What about my personal rights to privacy?

The public and Congress have raised privacy concerns regarding these searches. In response, among other things, DHS has undertaken to implement new procedures that include enhancement of recordkeeping processes, updated and continued training of officers and Special Agents who may engage in border searches of electronic devices, and the implementation of internal auditing procedures specific to the search, detention, and seizure of electronic devices. As previously noted, a PIA is being completed with regard to the privacy impact of the electronic search procedures by CBP and/or ICE. Furthermore, we are looking to improve mechanisms to better inform travelers of our policy, procedures and their rights with regard to the search of electronic devices at the border.

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 and ICE are vigilant about protecting sensitive information such as medical and business information. CBP and ICE abide by all laws regarding disclosure of personal information, including the Privacy Act, 5 U.S.C. § 552a. In addition, the Trade Secrets Act, 18 U.S.C. § 1905, prohibits Federal employees from disclosing, without lawful authority, business confidential information to which they obtain access as part of their official duties. CBP and ICE have strict policies and procedures that implement these constitutional and statutory safeguards. Finally, CBP and ICE have required training programs relating to these concepts on a yearly basis.

If during an examination, a passenger states that his/her items are privileged as a result of attorney-client privilege, then the CBP Officer or ICE Special Agent will appropriately notify his chain of command. In such cases, before a search commences, the CBP Office of the Chief Counsel or the ICE Office of the Principal Legal Advisor are to be contacted for advise and, in the course of an investigation, the appropriate United States Attorney's Office is to also be consulted.

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

Search: This is when CBP officers or ICE Special Agents examine documents, books, pamphlets, and other printed materials, as well as computers, disks, hard drives and other electronic or digital storage devices. Such examinations at the border (or its functional equivalent) require no suspicion.

Detention: This is when CBP or ICE detains 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, or authority to otherwise retain it, all copies of the information will be destroyed.

Seizure: This is when CBP or ICE determines that there is probable cause to believe a violation of law has occurred or that the information is evidence of a crime. Based on a review of information in documents or electronic devices encountered at the border or on

other facts and circumstances, CBP or ICE they may seize the originals and/or copies of relevant documents or devices, as authorized by law. CBP or ICE has the legal authority to retain such information consistent with applicable SORNs, policies, and laws.

Retention: Retention of documents also occurs where such is otherwise authorized by law (for example, copies of immigration related material may be retained for use in proceedings in Immigration court).

SEIZURES

Why would CBP or ICE seize a laptop?

CBP or ICE may seize a laptop only when there is probable cause to believe the laptop contains information that is evidence of a crime or that the laptop is otherwise subject to seizure and forfeiture under Federal law. A review of the data on laptop seizures in FY 2008 shows seizures were made for various reasons.

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

No. CBP records show that there have been 29 seizures of laptops since October 1, 2008. During this time CBP Officers encountered more than 134.8 million passengers. These seizures occurred as a result of the examination of the contents of the laptop or other electronic media in the possession of the traveler. This is about 0.001 percent of the total number of secondary examinations performed.

If a laptop has been seized, how and when would the traveler expect to get it back?

When a laptop is seized by either CBP or ICE, the traveler receives a "6051-S receipt" and a separate, mailed notice informing them that they have 30 days to file a petition with CBP to request that their laptop be returned. The notice includes an address and phone number so that the traveler may call for status updates.

Every time an original laptop is seized from a traveler, CBP or ICE issues the traveler a "6051-S" receipt for the merchandise. This receipt includes information on who to call for questions and updates. If ICE has interviewed the traveler, the ICE Special Agent will have given the traveler his or her contact information as well. If the laptop is seized as evidence, it will be returned to the owner after the completion of judicial proceedings, which could be of a civil or criminal nature. If the laptop is subject to forfeiture, CBP will send the owner a notice of seizure along with an explanation of the owner's rights to petition CBP for return of the laptop or to file a claim that will result in the Government instituting judicial proceedings to forfeit the laptop.