MEMORANDUM FOR: Directors, Field Operations  
Office of Field Operations

Director, Preclearance Operations

Director, Field Operations Academy  
Office of Training and Development

FROM: Executive Director  
Admissibility and Passenger Programs

SUBJECT: Packet Requirements

The purpose of this memorandum is to remind field personnel at Ports of Entry (POE) of the information reporting requirements consistent with CBP Directive 3340-02B, Section 6.9.11. This directive enumerates the requirements for examining, processing, and disposing of information.

Upon request of the and subject to applicable policies and procedures for the search of information, officers are required to make copies of including, but not limited to:

Even in the absence of a prior request by when a POE the POE officers must make a

For example: 

- FOR OFFICIAL USE ONLY — LAW ENFORCEMENT SENSITIVE —
has developed a comprehensive automated tracking system and the receipt or non-receipt of goods. When assembling a packet, it is important for POE personnel to provide copies of the best quality possible. Accurate review and analysis depends on clear, legible documents. POE staff should submit complete packets bound only with a clip or rubber band and should ensure that packets are not mixed or separated in the event the envelope or shipping container is damaged. It is recommended that the POE ship the packets (b)(2), (b)(7)(E).

Questions regarding the inspection process or during a secondary interview at the POE should be directed to (b)(2). Notification of processing delays or generic questions regarding packet preparation should be directed to (b)(2). Due to the sensitive nature of the information, failure to comply with these instructions may be reported to the appropriate Director of Field Operations for remedial action.
From: (b)(6), (b)(7)(C)
Sent: Thursday, September 25, 2008 8:28 AM
To: (b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)
Subject: RE: (b)(5)

(b)(6), (b)(7)(C)

From: (b)(5)
Sent: Thursday, September 25, 2008 8:24 AM
To: (b)(6), (b)(7)(C)
Cc: (b)(5), (b)(7)(C)
Subject: (b)(5)

(b)(6), (b)(7)(C)

(b)(2), (b)(6), (b)(7)(C)
Can I give you a call in the morning?

From: [REDACTED]
To: [REDACTED]
Cc: [REDACTED]
Sent: Wed Sep 24 18:01:26 2008
Subject: FW: [REDACTED]

Hey

[REDACTED]

Thanks.

From: [REDACTED]
Sent: Tuesday, September 23, 2008 9:40 AM
To: [REDACTED]
Subject: [REDACTED]

Expanded Powers to Search Travelers at Border Detailed

By Ellen Nakashima
Washington Post Staff Writer
Tuesday, September 23, 2008; A02

The U.S. government has quietly recast policies that affect the way information is gathered from U.S. citizens and others crossing the border and what is done with it, including relaxing a two-decade-old policy that placed a high bar on federal agents copying travelers’ personal material, according to newly released documents.

The policy changes, civil liberties advocates say, also raise concerns about the guidelines under which border officers may share data copied from laptop computers and cellphones with other agencies and the types of questions they are allowed to ask American citizens.

In July, the Department of Homeland Security disclosed policies that showed that federal agents may copy books, documents, and the data on laptops and other electronic devices without suspecting a traveler of wrongdoing. But what DHS did not disclose was that since 1986 and until last year, the government generally required a higher standard: Federal agents needed probable cause that a law was being broken before they could copy material a traveler was bringing into the country.

The changes are part of a broader trend across the government to harness technology in the fight against terrorism. But they are taking place largely without public input or review, critics said, raising concerns that federal border agents are acting without proper guidelines or oversight and that policies are being adopted that do not adequately protect travelers’ civil liberties when they are being questioned or their
belongings searched.

"For 20 years the government has at least implicitly recognized there were some First Amendment restrictions on reading and copying documents," said Shirin Sinnar, a staff attorney with the Asian Law Caucus, which along with the Electronic Frontier Foundation sued the government under the Freedom of Information Act for disclosure of border search policies. "It's disturbing now that the government has jettisoned that policy in favor of one that violates First Amendment rights."

DHS spokeswoman Amy Kudwa said the updating of policies reflects an effort to be more transparent. In an e-mail, she wrote that the decision of U.S. Customs and Border Protection (CBP) "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 requiring suspicion of a particular traveler.

The 1986 policy was issued after a lawsuit was filed by a group of activists returning from Nicaragua who had their diaries, datebooks and other personal papers seized and photocopied by customs officers and shared with the FBI. The government argued that the customs agency had the right to enforce a law against importing subversive literature.

"Essentially they were using that as a pretext to do intelligence gathering on critics of our policies in Nicaragua," said David D. Cole, a Georgetown University law professor who was then a lawyer at the Center for Constitutional Rights, representing the activists suing the government in Heidy v. U.S. Customs Service.

To set guidelines on document searches, the agency issued the 1986 directive that made clear that its officers "as a general rule... should not read personal correspondence." But, the policy noted, officers had the authority to scan material for evidence of violation of laws pertaining to copyright, sedition and contraband. With reasonable suspicion of a violation, they could detain the material. With probable cause of a violation, they could seize and copy it.

In July 2007, the government dropped the requirement that there be reasonable suspicion to review material but specified that the review had to take place in connection with laws enforced by CBP, according to a copy of a policy the groups obtained.

Then, this July, the government issued its broadest policy to date regarding information searches at the border, allowing documents and electronic devices to be detained for an unspecified period. Moreover, they may now be copied without any suspicion of wrongdoing, the lowest legal standard.

"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," Kudwa said.

But Marcia Hofmann, staff attorney for the Electronic Frontier Foundation, said that laptop computers may contain "a massive amount of private information such as personal e-mails, financial data or confidential business records" and that the government should not violate travelers' constitutional rights in the name of national security.

There is apparently wide interest among other government agencies in CBP's ability to collect

(b)(2), (b)(6), (b)(7)(C)
information, according to a July 11, 2007, e-mail obtained by the groups. The e-mail originated from the agency's New York field office. "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 Heidy decision barred customs officers from sharing information they suspected was seditious with other federal agencies unless the agencies abided by CBP's restrictions on data retention. But the July policy allows the agency to share data obtained at the border if there is suspicion that a law enforced by it is being violated.

Cole said the government's search authority at the border is very broad, "so it is important that it not be turned into a loophole by which other law enforcement agencies, which are not permitted to conduct searches without probable cause or reasonable suspicion, are able to avoid the constitutional limits on their authority."

Customs officers are trained to know under what circumstances sensitive law enforcement information may be shared and with whom, DHS spokesman Russ Knocke said.

Over the past several years, the Asian Law Caucus and other civil liberties groups have reported a surge in complaints from travelers who have been questioned about their religious practices and political leanings. Many of the travelers say they have had their laptops or phones searched.

Yasir Qadhi, a 33-year-old Houston native who studied in Saudi Arabia from 1995 to 2005 and is pursuing a doctorate in Islamic studies at Yale University, said he is questioned every time he reenters the United States. He said he is routinely asked which mosques he has prayed in, what charities he donates to, what lectures he has delivered, what the lectures are titled. If he has notes, he said, they are photocopied.

In March 2006, when driving home to New Haven, Conn., from Toronto, he said, he was detained with his wife and three children at the border for 5 1/2 hours. The agents, he said, asked about religion, and, noting his Saudi studies, asked him for classmates' names and whom he corresponded with in the United States.

They also detained his cellphone.

Then, this spring, an agent in the FBI's New Haven field office asked him to come by. Qadhi said the agent cited the March 2006 stop and said, "We went through your personal diary in your phone, and we discovered these numbers on there, and we want to know your relationship with these specific individuals."

Qadhi said: "And they went through each one of them."

Knocke said he could not comment on an individual case. He said customs officers do not racially profile in any way but have the authority to "take and consider evidence concerning the privilege" of any person to enter the United States.

Nathan A. Sales, former DHS deputy assistant secretary for policy development, said that "in some instances, you can imagine it would be appropriate to ask questions" such as those asked of Qadhi. "But when you do, you're playing with fire."

(b)(2), (b)(6), (b)(7)(C)
Sales, a George Mason University law professor, said: "If you want to ask questions about a person's churchgoing or charitable contributions, you need to take steps to ensure it doesn't stray from legitimate questions to harassment. You need to have a clearly established policy that these sorts of questions are only asked in certain circumstances, and only when we have some indication to believe that a particular mosque or a particular charity might have some sort of terrorist tie."

Qadhi said he feels "frustrated" by a system that he thinks will never tell him what list he is on so that he can get off it. "I'm treated like a second-class citizen, and there's absolutely nothing I can do," he said. "This is simply not the America I grew up in."

Staff researcher Julie Tate contributed to this report.
CONFIDENTIALITY NOTICE: This electronic transmission and/or any/all attachments are to be considered Sensitive But Unclassified (SBU) / For Official Use Only (FDOU) / Law Enforcement Sensitive (LES), and are to be handled and disseminated accordingly.

This electronic transmission, including any attachments, is for the sole use of the intended recipient(s) and may contain sensitive but unclassified information or Privacy Act data and is protected from disclosure under the Freedom of Information Act, 5 USC 552. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

From: (b)(6), (b)(7)(C)
Sent: Friday, February 15, 2008 09:26
To: (b)(6), (b)(7)(C)
Subject: FW: CBP Policy on Laptop Searches

(b)(5)

(b)(6), (b)(7)(C)
I work for a P.L. firm in San Diego. The work is interesting and varied. As I mentioned yesterday, we have a multinational company client whose employees often travel to foreign destinations on business with their company laptops. Recently upon returning to the U.S. at airports and land ports of entry, a few have encountered instances where CBP Inspectors reportedly inspected their laptops and examined the actual software and hard drive contents. The company is concerned that their proprietary and protected trademark info could be compromised or possibly deleted.

The company desires to know CBP policy re laptop inspections and exams of internal data and the circumstances under which laptops can possibly be seized and/or the software and hard drive data be examined or copied by CBP. The company will then consider internal company policy changes to adjust to CBP policy in order to avoid the compromise of their proprietary and protected trademark data.

Would appreciate any policy info that you can share to pass on to the company. The company is not looking to complain. It desires to comply with CBP requirements, but wants any understanding of the existing policy and circumstances under which more in depth inspections of laptops may occur.

Gracias
From: (b)(6), (b)(7)(C)
Sent: Tuesday, August 05, 2008 3:55 PM
To: (b)(6), (b)(7)(C)  
Subject: FW: Searches of Attorney Laptops on Reentry
FYI – Please see the message below sent to [REDACTED] in response to his questions about CBP’s laptop searches.

From: (b)(6), (b)(7)(C)
Sent: Tuesday, August 05, 2008 3:53 PM
To: (b)(6), (b)(7)(C)
Subject: RE: Searches of Attorney Laptops on Reentry

Dear [REDACTED]

I was forwarded your message sent to the Chief Counsel of U.S. Customs and Border Protection (CBP) regarding searches of laptops. I wanted to let you know that CBP recently posted a policy on this issue, which can be found at [http://www.cbp.gov/linkhandler/cgov/travel/admissability/search_authority.ctt/search_authority.pdf](http://www.cbp.gov/linkhandler/cgov/travel/admissability/search_authority.ctt/search_authority.pdf). In particular, I would like to direct your attention to page 4 of this policy, which contains a provision concerning attorney-client privileged material.

Regards

From: (b)(6), (b)(7)(C)
Sent: Tuesday, April 21, 2009 5:50 PM
To: (b)(6), (b)(7)(C)
Cc: 
Subject: Searches of Attorney Laptops on Reentry

Dear [REDACTED]

As an attorney who travels abroad, albeit infrequently, and invariably performs client-related work while traveling, I was concerned to read of the random seizures of laptop computers of returning U.S. citizens “for examination.” (See, e.g., [http://www.latimes.com/business/la-fi-laptops26-2008jun26.0,4415017.story](http://www.latimes.com/business/la-fi-laptops26-2008jun26.0,4415017.story) ) I teach MCLE courses, and write about technology-related issues in legal profession publications, and therefore have an additional interest in these matters.

Under California law, an attorney has the duty “to maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.” (Cal. Bus. & Prof. Code § 6068(e)(1).) This duty is far broader than the attorney-client privilege. In addition to the duty under Section 6068(c),

the custodian of materials protected by an evidentiary privilege owes a duty to the holder of the privilege to claim the privilege and to take actions necessary to ensure that the materials are not
disclosed improperly. (E.g., Evid. Code, §§ 955 [attorney], 995 [physician], 1015 [psychotherapist]; ....) Even if the custodian is suspected of a crime, when privileged materials in the custodian's possession are seized pursuant to a search warrant, he or she still owes a duty to take appropriate steps to protect the interest of the privilege holders in not disclosing the materials to law enforcement authorities or others.

(People v. Superior Court, 25 Cal.4th 703, 107 Cal.Rptr.2d 323, 23 P.3d 563 (2001).) These principles are recognized by federal courts. (See, e.g., Klitzman, Klitzman & Gallagher v. Krui, 744 F.2d 955 (3rd Cir. 1984).)

As a result, when searches of an attorney's files or records is to be conducted, a special master is appointed at the time a search warrant issues to supervise compliance with the search warrant, to conduct the search if the attorney fails to comply, to seal and take custody of any materials the attorney states should not be disclosed (including privileged materials), and to present those materials to the court for decision regarding the claims of the attorney (including claims of privilege). (Cal. Pen. Code § 1524 (c).) The same rules apply to searches of records of a physician, a psychotherapist, and a member of the clergy. (Ibid.) As you know, state laws of privilege govern in the federal setting. In addition, there are federal regulations addressing the searching of privileged materials. (See 28 C.F.R. §§ 59.1 et seq., esp. § 59.4.)

In his written testimony presented last month to the Constitution Subcommittee of the Senate Committee on the Judiciary, Deputy Commissioner Ahern stated:

In regards to the privacy of these searches, CBP officers conduct their work in a manner designed to adhere to all constitutional and statutory requirements, including those that are applicable to privileged, personal, and business confidential information. The Trade Secrets Act prohibits federal employees from disclosing, without lawful authority, business confidential information to which they obtain access as part of their official duties. Moreover, CBP has strict policies and procedures that implement constitutional and statutory safeguards through internal policies that compel regular review and purging of information that is no longer relevant. CBP will protect information that may be discovered during the examination process, as well as private information of a personal nature that is not in violation of any law.

(Statement of Jayson P. Ahern, Deputy Commissioner, U.S. Customs and Border Protection, Department of Homeland Security, Before The Senate Committee on the Judiciary Constitution Subcommittee, "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel," Washington, DC, June 25, 2008 - http://www.cbp.gov/xp/cgov/newsroom/congressional_test/laptop_searches.xml.) The news articles and the testimony of Deputy Commissioner Ahern raise the following questions:

- Since even trusted travelers under the Global Entry system can chosen for selective or random examination, when conducting a random examination of the contents of a laptop computer carried by an attorney or other professional obliged to preserve privileged and confidential information, does CBP utilize a procedure analogous to that required by Section 1524(c) of the California Penal Code?
- In the face of the multitude of data breaches experienced by agencies of the Government over the past several years, do the "strict policies and procedures" referred to by Deputy Commissioner Ahern include severely restricted access to privileged and work-product information, the encryption of all such information on CBP systems, and MilSpec-level deletion when such information is purged?
As one attorney to another, I would appreciate your response to these questions. Thank you in advance for your time and consideration.

Very truly yours,

(b)(6), (b)(7)(C)

(b)(2), (b)(6), (b)(7)(C)
Laptop Seizures

C-Span is running a story on Monday regarding CBP’s authority to seize laptop computers.

Talking Points

- CBP is pleased that its longstanding search authority at the border, including the authority to search, without suspicion, laptop computers for violations of law, has been upheld by the Court of Appeals for the Ninth Circuit.

- This decision overturns a lower court ruling in favor of an individual who was charged with child pornography and related criminal offenses after CBP Officers found child pornography on his laptop computer on his arrival at Los Angeles International Airport from the Philippines.

- CBP’s primary mission is to protect the American public from terrorists and terrorist weapons while facilitating legitimate trade and travel. CBP Officers work diligently to treat all travelers in a professional and courteous manner while determining if an individual is entering the country legally. Officers also have the responsibility to check items such as laptops and other personal electronic devices to ensure that any item brought into the country complies with applicable law and is not a threat to the American public.
- Laptop computers and other personal electronic devices may be detained for violations of law including child pornography, intellectual property offenses, ties to terrorism, or other violations of law.

- CBP Officers are dedicated to protecting the civil rights of all travelers. It is not CBP's intent to subject legitimate business travelers to undue scrutiny, but to ensure the safety of the American public.
Talking Points

CBP's longstanding search authority at the border has been unanimously upheld by the courts to allow our officers to lawfully search laptops to ensure that any item brought into the country safe and illegal and is not a threat to the American public.

Laptop computers may be detained for violations of criminal law such as child pornography, ties to terrorism, intellectual property rights offenses and other violations of law.

It is not CBP's intent to subject legitimate business travelers to undue scrutiny, but to ensure the safety of the American public. CBP officers are dedicated to protecting the privacy and civil rights of all travelers.