NOT RESPONSIVE

[redacted]

From: (b)(6) & (b)(7)(C)
Sent: Friday, February 08, 2008 11:32 AM
To: (b)(6) & (b)(7)(C)

[redacted]

Subject: FW: INFO: CBP support of non [redacted] requests for information (b)(2) & (b)(7)(E)

(b)(2) + (b)(7)(E)

Port Directors,

As you can see, the lawsuit filed against CBP in San Francisco has made all the newspapers. The DFO would like you to make sure that all your officers conducting searches of electronic devices are following the guidance disseminated by the Field Office in November (see below). Please discuss this issue during your daily musters and emphasize the importance of developing the appropriate level of suspicion before conducting a search.

[redacted] – (b)(6) + (b)(7)(C)

- **San Francisco Chronicle-Homeland Security sued for not divulging info** (Neutral/ Negative)

Nabila Mango, a therapist who works in San Francisco, flew home in December after a trip to the Middle East and says customs agents detained her and asked her to identify everyone she had met and all the places she'd slept.

Amir Khan, a tech consultant from Fremont, says he's questioned for hours each time he

(b)(2) [redacted]

returns from abroad and has been asked whether he hates the U.S. government.

After receiving more than 20 such complaints in the past year, mostly from South Asians and Muslims, two legal organizations sued the Homeland Security Department on Thursday for information on its policies of questioning and searching returning travelers.

"When the government searches your books, peers into your computer and demands to know your political views, it sends the message that free expression and privacy disappear at our nation's doorstep," attorney Shirin Sinnar of the Asian Law Caucus said at a news conference after filing the suit in U.S. District Court in San Francisco.

The Asian Law Caucus and the Electronic Frontier Foundation said they asked Homeland Security's Customs and Border Protection division for its policies Oct. 31 and have yet to receive any documents, despite a 20-day deadline for a response from the government under the Freedom of Information Act.

The groups want to know what policies guide customs agents in asking political or religious questions, what happens when a traveler refuses to answer or wants a lawyer, and what standards exist for agents who want to search or copy material from laptop computers, cell phones and other electronic devices.

Courts have allowed federal agents more leeway in searches at borders and airports than elsewhere, and some rulings have allowed customs agents to search laptops and cell phones without evidence the devices' owners have done anything wrong. Sinnar said she considers the searches of electronic devices legally questionable, and that singling out travelers by race or religion would raise serious constitutional concerns.

Homeland Security spokeswoman Laura Keehner declined to comment on the lawsuit but said laptops can be seized and searched "when they contain information in violation of U.S. criminal law" - for example, if they are being used in terrorism, drug smuggling or child pornography. She would not discuss agents' inquiries into travelers' politics or religion.
http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/02/08/BAVQUUAJ8.DTL

- **Washington Post-Encrypted Laptop Poses Legal Dilemma** (Neutral)

BURLINGTON, Vt. -- When Sebastien Boucher stopped at the U.S.-Canadian border, agents who inspected his laptop said they found files containing child pornography.

But when they tried to examine the images after his arrest, authorities were stymied by a password-protected encryption program.

Now Boucher is caught in a cyber-age quandary: The government wants him to give up the password, but doing so could violate his Fifth Amendment right against self-incrimination by revealing the contents of the files.

Experts say the case could have broad computer privacy implications for people who cross borders with computers, PDAs and other devices that are subject to inspection.

"It's a very, very interesting and novel question, and the courts have never really dealt with it," said Lee Tien, an attorney with the Electronic Frontier Foundation, a San Francisco-based group focused on civil liberties in the digital world.

For now, the law's on Boucher's side: A federal magistrate here has ruled that forcing Boucher to surrender the password would be unconstitutional.

The case began Dec. 17, 2006, when Boucher and his father were stopped at a Derby Line, Vt., checkpoint as they entered the U.S.

Boucher, a 30-year-old drywall installer in Derry, N.H., waived his Miranda rights and cooperated with agents, telling them he downloads pornography from news groups and sometimes unknowingly acquires images that contain child pornography.

Boucher said he deletes those images when he realizes it, according to an affidavit filed by Immigration and Customs Enforcement.

At the border, he helped an agent access the computer for an initial inspection, which revealed files with names such as "Two year old being raped during diaper change" and "pre teen bondage," according to the affidavit.
http://www.washingtonpost.com/wp-dyn/content/article/2008/02/07/AR2008020702378.html

---

From: (b)(6) & (b)(7)(C) [redacted]
Sent: Monday, November 05, 2007 8:13 AM
To: (b)(6) & (b)(7)(C) [redacted]

(b) (2) [redacted]

(b) (2) [redacted]

Cc: (b)(6) & (b)(7)(C) [redacted]

Subject: INFO: CBP support of non [redacted] requests for information (b)(2) & (b)(7)(E) [redacted]

(b)(2) + (b)(7)(E)

(b) (2) [redacted]

To All,

The Field Office received a question from a Port of San Francisco [redacted] Liaison regarding requests from the [redacted] for assistance on matters involving (b)(2) & (b)(7)(E) [redacted]. Questions arise when certain material or documentation is requested. The issue can be especially sensitive for CBP with regard to (b)(2) & (b)(7)(E) [redacted]. The guidance for dealing with such requests is as follows. Please note that full instructions are available in Assistant Commissioner Jayson P. Ahern's Memorandum and Interim Procedures dated July 5, 2007, as well as in CBP Directive 3340-006A, Procedures for Examining Documents and Papers.

Examinations may be performed by CBP on subjects of interest at the border or functional equivalent of the border (FEB). Requests from the (b)(2) & (b)(7)(E) [redacted] must be coordinated through the Port's chain of command with the Field Office (ADFO-Border Security). Such requests, with or without a (b)(2) & (b)(7)(E), may require coordination, by the originating agency, with (b)(2) & (b)(7)(E) [redacted].

(b)(2) + (b)(7)(E)

[redacted]

(b)(2) & (b)(7)(E) [redacted]

documents and electronic devices may be reviewed absent individualized suspicion in the course of administering laws enforced by CBP. Documents and information from electronic devices or electronic storage media may be copied or transmitted without individualized suspicion if technical assistance is necessary to determine the existence of a violation (i.e. translation support). Documents and information copied or transmitted to receive this assistance must be returned to CBP as expeditiously as possible. Documents and information also may be copied or transmitted if either of the following conditions is met:

- There is reasonable suspicion to believe the subject is involved in or the material in question may relate to terrorism or other illegal activity, or
- (b)(2) & (b)(7)(E) [redacted] consents to the copying or transmission.

Reasonable suspicion may be developed from a review of all factors like the examination and interview, available investigative information, etc. Officers should not copy or transmit information purely on the basis of a request to copy from an outside agency. If copies are made and the outside agency requests to retain or disseminate them, officers should follow the appropriate procedures to turn the information over to the requesting agency (CF 6051-chain of custody, etc.).

(b)(2) + (b)(7)(E)

[redacted] documents and information from electronic devices or electronic storage media should not be reviewed longer than a "glance" unless:

- There is reasonable suspicion to believe the subject is involved in or the material in question may relate to terrorism or other illegal activity, or
- (b)(2) & (b)(7)(E) consents to the further inquiry.

Documents and information should not be copied without:

- Consent from the subject,
- Probable cause to believe the document or information is subject to seizure, or
- A court order/(b)(2) & (b)(7)(E).

The requesting agency may be provided appropriate exam result information ((b)(2) & (b)(7)(E), etc) by completing the required request for information and following the appropriate dissemination procedures.

Please disseminate the information provided to all appropriate personnel.

(b)(6) & (b)(7)(C)
Border Security Coordinator
(b)(6) & (b)(7)(C)

From: (b)(6) & (b)(7)(C)
Sent: Thursday, March 06, 2008 12:30 PM
To: (b)(6) & (b)(7)(C)
Subject: FW: INFO: CBP support of non [redacted] requests for information (b)(2) & (b)(7)(E)

(b)(2) + (b)(7)(E)

From: (b)(6) & (b)(7)(C)
Sent: Tuesday, February 12, 2008 12:36 PM
To: (b)(6) & (b)(7)(C)

[redacted]

Subject: FW: INFO: CBP support of non [redacted] requests for information (b)(2) & (b)(7)(E)

(b)(2) + (b)(7)(E)

Port Directors,

The examination of electronic devices has become a very HOT topic in DC (all the way to the White House). Effective immediately, the DFO wants you to establish the following procedures:

1. All searches of electronic media will require supervisory approval.
2. Detention of electronic media will require approval by the Port Director.

I cannot over emphasize the importance of establishing the appropriate level of suspicion before conducting an examination of an electronic media.
Please feel free to call if you have any questions.

[redacted] — (b)(6) + (b)(7)(C)

From: (b)(6) & (b)(7)(C)
Sent: Friday, February 08, 2008 11:32 AM
To: (b)(6) & (b)(7)(C)

[redacted]

(b)(2) + (b)(7)(E)

Subject: FW: INFO: CBP support of non [redacted] requests for information (b)(2) & (b)(7)(E)

Port Directors,

As you can see, the lawsuit filed against CBP in San Francisco has made all the newspapers. The DFO would like you to make sure that all your officers conducting searches of electronic devices are following the guidance disseminated by the Field Office in November (see below). Please discuss this issue during your daily musters and emphasize the importance of developing the appropriate level of suspicion before

conducting a search.

(b)(6) + (b)(7)(C)

From: (b)(6) & (b)(7)(C)
Sent: Monday, November 05, 2007 8:13 AM
To: (b)(6) & (b)(7)(C)

Subject: INFO: CBP support of non requests for information (b)(2) & (b)(7)(E)
(b)(2) + (b)(7)(E)

(b)(2)

To All,

(b)(2) + (b)(7)(E)

The Field Office received a question from a Port of San Francisco Liaison regarding requests from the for assistance on matters involving (b)(2) & (b)(7)(E). Questions arise when certain material or documentation is requested. The issue can be especially sensitive for CBP with regard to (b)(2) & (b)(7)(E). The guidance for dealing with such requests is as follows. Please note that full instructions are available in Assistant Commissioner Jayson P. Ahern's Memorandum and Interim Procedures dated July 5, 2007, as well as in CBP Directive 3340-006A, Procedures for Examining Documents and Papers.

Examinations may be performed by CBP on subjects of interest at the border or functional equivalent of the border (FEB). Requests from (b)(2) & (b)(7)(E) must be coordinated through the Port's chain of command with the Field Office (ADFO-Border Security). Such requests, with or without a (b)(2) & (b)(7)(E), may require coordination, by the originating agency, with (b)(2) & (b)(7)(E)

(b)(2) + (b)(7)(E)

(b)(2) & (b)(7)(E)

documents and electronic devices may be reviewed absent individualized suspicion in the course of administering laws enforced by CBP. Documents and information from electronic devices or

electronic storage media may be copied or transmitted without individualized suspicion if technical assistance is necessary to determine the existence of a violation (i.e. translation support). Documents and information copied or transmitted to receive this assistance must be returned to CBP as expeditiously as possible. Documents and information also may be copied or transmitted if either of the following conditions is met:

- There is reasonable suspicion to believe the subject is involved in or the material in question may relate to terrorism or other illegal activity, or
- (b)(2) & (b)(7)(E) consents to the copying or transmission.

Reasonable suspicion may be developed from a review of all factors like the examination and interview, available investigative information, etc. Officers should not copy or transmit information purely on the basis of a request to copy from an outside agency. If copies are made and the outside agency requests to retain or disseminate them, officers should follow the appropriate procedures to turn the information over to the requesting agency (CF 6051-chain of custody, etc.).

(b)(2)+(b)(7)(E)

[redacted] documents and information from electronic devices or electronic storage media should not be reviewed longer than a "glance" unless:

- There is reasonable suspicion to believe the subject is involved in or the material in question may relate to terrorism or other illegal activity, or
- (b)(2) & (b)(7)(E) consents to the further inquiry.

Documents and information should not be copied without:

- Consent from the subject,
- Probable cause to believe the document or information is subject to seizure, or
- A court order (b)(2) & (b)(7)(E)

The requesting agency may be provided appropriate exam result information ((b)(2) & (b)(7)(E), etc) by completing the required request for information and following the appropriate dissemination procedures.

Please disseminate the information provided to all appropriate personnel.

(b)(6) & (b)(7)(C)
Border Security Coordinator
(b)(6) & (b)(7)(C)