

Electronic Frontier Foundation

September 30, 2008

VIA EMAIL

The Honorable Russell D. Feingold
Committee on the Judiciary
United States Senate
Washington, DC 20510-6275

Dear Senator Feingold,

Thank you for your July 15, 2008 letter in response to Senior Staff Attorney Lee Tien's testimony at the United States Senate Judiciary Committee Subcommittee on the Constitution hearing regarding "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel."

Enclosed please find responses to the written questions that accompanied your letter.

We look forward to continuing to work with the Committee to address the civil liberties threats posed by suspicionless border searches. If we can provide additional assistance on this or any other matter, please do not hesitate to let us know.

Sincerely,

Jennifer Granick
Civil Liberties Director

Enclosure

Senate Judiciary Committee
Subcommittee on the Constitution
Hearing on "Laptop Searches and Other Violations of Privacy Faced by Americans Returning From Overseas Travel"
Wednesday, June 25, 2008

Answers of Lee Tien
to Questions Submitted by U.S. Senator Russell D. Feingold

1. **Five days after the Constitution Subcommittee held this hearing, DHS posted a blurb entitled "CBP Laptop Searches" on its website: http://www.dhs.gov/journal/leadership/2008/06/cbp-laptop-searches.html. The blurb notes three examples of cases in which laptop searches revealed "violent jihadist material, information about cyanide and nuclear material, video clips of improvised Explosive Devices (IEDs), pictures of high-level Al-Qaeda officials, and other material associated with people seeking to do harm to our country." Notably, only one of these examples involved a U.S. citizen, despite the fact that the issue currently under debate – and the primary focus of the hearing – is the rights of Americans at the border. In that example, the laptop search occurred <u>after</u> an inspection of the traveler's baggage "revealed approximately $79,000 in unlawful U.S. currency." Although DHS states that the laptop search revealed "information about cyanide and nuclear material," the individual apparently pleaded guilty only to "bulk cash smuggling and making false statements," and was sentenced to 12 months in prison.**

    a. **Would a "reasonable suspicion" requirement have prevented this search from occurring?**

Answer: No, a "reasonable suspicion" requirement would not have prevented this search from occurring. Prior to the laptop search, the individual had already been singled out for suspicion based on a law enforcement tip that he was smuggling cash, and a routine luggage search had revealed $79,000 in unlawful U.S. currency. These are circumstances that meet the "reasonable suspicion" standard, as past court cases construing "reasonable suspicion" demonstrate. All information available to a law enforcement officer must lead officers to suspect that the specific person in question is engaged in wrong doing. For example, in *United States v. Cortez*, 449 U.S. 411, 417 (1981), the Supreme Court held that "an objective manifestation that the person stopped is . . . engaged in criminal activity" creates reasonable suspicion justifying further investigation. The smuggling tip coupled with the individual's possession of $79,000 in unlawful currency is a manifestation of criminal activity rising to the level of reasonable suspicion sufficient to justify a laptop search.

b. Do the circumstances of this case suggest to you that the laptop search resulted in the apprehension and incapacitation of a dangerous terrorist?

Answer: No, the description of this case provided by CBP does not indicate that the laptop search resulted in the apprehension and incapacitation of a dangerous terrorist. Rather, the individual at issue was detained and convicted based on the discovery of illegal currency in his baggage. CBP's description of the case states that the search of the individual's laptop computer revealed information about cyanide and nuclear material. This fact alone does not prove that the man possessed this information for an improper purpose or that he was a terrorist. Tellingly, the prosecution apparently did not rely on information obtained from the laptop to prosecute the individual. CBP's description of the case suggests that he was convicted on the basis of the unlawful U.S. currency, not the results of the laptop search.

c. Both of the DHS's examples regarding non-citizens involved searches that took place after the individual was selected for secondary screening – in one case, "based on the individual's behavior and questions by CBP officers." Based on the information DHS put in its blurb, is there any basis for concluding that these searches that would have been impossible under a "reasonable suspicion" requirement?

Answer: No, there is no basis to conclude that the searches described by DHS would have been impossible under a "reasonable suspicion" requirement. At least one of the cases clearly involved circumstances that met the "reasonable suspicion" requirement as defined by the courts. The individual was referred to secondary screening "based on his behavior and questions by CBP officers." Past judicial opinions have held that suspicious behavior and responses to questioning like those cited in DHS's example may constitute "reasonable suspicion." For example, in *United States v. Montoya De Hernandez*, 473 U.S. 531, 542 (1985), the Supreme Court determined that an individual's responses to customs officials' questions, including an "implausible story" she recounted to them, "clearly supported a reasonable suspicion" that the individual was engaged in drug smuggling. The DHS blurb does not indicate why the other individual was singled out for secondary screening, but the reasons that he was selected out for additional screening could also support a finding of reasonable suspicion.

2. The DHS blurb on "CBP Laptop Searches" gives two examples of cases in which border laptop searches revealed "intellectual property rights violations and child pornography." In the first example, based on prior coordination with Immigration and Customs Enforcement, customs agents searched the laptop of a Canadian national who was "suspected of stealing proprietary software programs from a U.S. company and attempting to sell the software to the People's Republic of China." In the second example, customs agents searched the laptop of an individual (DHS does not state the

individual's nationality) after the individual "exhibited nervous behavior when questioned about the purpose of travel to Manila" and "failed to provide consistent answers about his occupation."

Would a reasonable suspicion requirement have prevented either search from occurring?

Answer: No, DHS's characterization of these cases suggest that a reasonable suspicion requirement would not have prevented the first search described by DHS from occurring, and probably would not have prevented the second search, either. The few facts available about these cases suggest that they both involved numerous circumstances to support the customs agents' belief that the travelers had committed wrongdoing prior to a search of their laptops. This level of suspicion makes these cases comparable to *United States v. Montoya de Hernandez*, in which the Supreme Court found reasonable suspicion to detain and search the alimentary canal of a traveler based a number of facts including her frequent travel between a well known drug zone, questionable responses about the purpose of travel, and the unusual tautness of her stomach. *Montoya de Hernandez*, 473 U.S. 531 (1985).

In the first case described by DHS, customs agents already suspected that the individual crossing the border was stealing proprietary software to sell to China before they searched the individual's laptop. The agents appear to have had at least as much information to justify the search as the agents did in *Montoya de Hernandez*, where there was no reason to suspect the traveler of wrong doing until she arrived at the airport and gave an implausible story about the contents of her luggage and her purpose for being in the United States. *Montoya De Hernandez*, 473 U.S. at 542.

DHS's second example includes very little detail, though the individual appeared nervous and during questioning failed to provide consistent answers about his occupation and purpose of travel. Even these few facts demonstrate that the situation was likely comparable to that in *Montoya De Hernandez,* though more information about the case would be helpful in making that assessment. The traveler's implausible story, in combination with other factors may well have risen to the level of reasonable suspicion.

3. The DHS website entry on "CBP Laptop Searches" states that "CBP officers adhere to strict constitutional and statutory requirements." In its voluminous court briefs and filings arguing that the First and Fourth Amendments pose no obstacle to suspicionless laptop searches, has DHS identified or conceded any constitutional or statutory limitations on its ability to search laptops at the border?

Answer: No. In our review of all the DHS filings in *United States v. Arnold,* a 2008 Ninth Circuit Court of Appeals decision holding that no reasonable

suspicion is required for laptop searches, the United States has not identified or conceded any constitutional or statutory limitations on the government's ability to search laptops at the border. On the contrary, the government argues that DHS has "plenary authority" to conduct suspicionless searches of personal property at the border. *See, e.g.,* Government's Opening Brief at 17, *United States v. Arnold,* 523 F.3d 941 (9th Cir. 2008) (No. 06-50581). The government has argued that border searches constitute an exception to the Fourth Amendment's restrictions, and that statutes outlining the authority of customs officials "should be construed as broadly as possible" in order to include computers in the category of "containers" that customs officials can search without warrant or suspicion. Brief of the United States at 11, *United States v. Ickes,* 393 F.3d 501 (4th Cir. 2005) (No. 03-4907). CBP recently went so far as to state that the agency may seize digital documents that are encrypted or in languages other than English and ask other federal agencies to translate or decrypt information in documents or on digital devices without individualized suspicion. See Policy Regarding Border Search of Information, Customs and Border Protection at 2 (July 16, 2008), *available at* Http://www.cbp.gov/linkhandler/cgov/travel/admissability/search_authority.ctt/search_authority.pdf.

4. **Your organization filed a Freedom of Information Act (FOIA) request asking DHS to disclose its "policies and procedures on conducting searches and duplicating files from laptop computers, MP3 players, digital cameras, cell phones, and other electronic devices." The written testimony that DHS submitted the night before the June 25 hearing purports to provide, quote, "specific information" about these policies. Having reviewed that testimony, do you feel that this testimony obviates the need for you to pursue your FOIA claim?**

Answer: No, the information provided in DHS's written testimony does not obviate the need to pursue the FOIA request filed jointly by EFF and the Asian Law Caucus, or the subsequent lawsuit we filed due to the agency's failure to respond to our request in a timely manner. The testimony does not answer many of the questions that remain about DHS's policies and procedures for searching digital devices, including:

- How do border agents decide that a certain digital device will be searched?
- What procedures and policies regulate such searches?
- Under what circumstances do border agents copy and retain information on digital devices, and do they duplicate everything on a device, or only certain files?
- What policies and procedures regulate later searches of digital information for purposes other than those for which it was initially retained?

- Is digital information collected during a border search ever expunged? Under what circumstances?

We hope that our FOIA lawsuit will continue to help to uncover the answers to these vital questions, which are currently not in the public record.

5. In his opening statement, Senator Brownback stated, "As a legal matter, it seems clear to me that Government officials do have the right under the Constitution to search laptop computers and similar devices without probable cause or reasonable suspicion at the border." As support for this assertion, he cited a customs statute that Congress passed two months before proposing the Bill of Rights, which gave officials the power to search any ship or vessel "in which <u>they shall have reason to suspect</u> any goods, wares, or merchandise subject to duty shall be concealed."

Doesn't this statute indicate that Congress *did* intend to limit border searches to cases in which reasonable suspicion was present?

Answer: While the plain language of this 1789 statute shows that the first Congress believed reasonable suspicion was required for border searches, the Supreme Court cited this statute in a 1977 case finding no such requirement. Scholars may question whether statutory language supports or undermines the Supreme Court's conclusion, especially because historical evidence suggests that searches in maritime contexts such as aboard ships were considered different from searches that occurred on land.

The plain language of the Customs Act of 1789, section 24, stated that customs officials must have *reason to suspect* that goods subject to duty were concealed before officials could search and seize the goods on a ship. This first Congress acted in the same spirit when, two months later, it passed the Fourth Amendment to protect individuals against arbitrary and capricious government searches.

However, in his testimony quoting the Customs Act, Senator Brownback cited *United States v. Ramsey*, 431 U.S. 606 (1977), in which the Supreme Court concluded that routine border searches are per se reasonable due to the fact that they occur at the border, since they serve to protect the country from the entry of contraband. *Id.* at 619. In the majority opinion, Justice Rehnquist stated that that language of the 1789 customs statute was an acknowledgement of plenary customs power, not a "reasonable suspicion" limitation, "differentiated from the more limited power to enter and search 'any particular dwelling-house, store, building, or other place . . .' where a warrant upon 'cause to suspect' was required." *Id.* at 616. In concurrence, Justice Powell argued that the case should have been decided only on reasonableness grounds since the majority agreed that the customs official had a reasonable suspicion that the international letter in question carried contraband. *Id.* at 625. In dissent, Justice Stevens, joined by two other Justices, said suspicionless border searches were "abhorrent to the tradition

of privacy and freedom to communicate protected by the Bill of Rights." *Id.* at 626.

Debate over the exact meaning of the phrase "reason to suspect" in the Custom Act may be misplaced. In his extensive analysis of the historic roots of the Fourth Amendment, Professor Thomas Davies argues that ships and maritime customs were governed by admiralty law, a branch of civil law, and were thus considered distinct from the persons, houses, papers, and effects protected by the Fourth Amendment. Thomas Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 605-06 (1999). Davies persuasively argues that the Framers intended the Fourth Amendment to eliminate general warrants rather than prohibit unreasonable searches because they felt that warrantless searches were inherently unreasonable. *Id.* at 551. *See also California v. Ciraolo*, 476 U.S. 207, 225 (1986) ("Warrantless searches are presumptively unreasonable, though the Court has recognized a few limited exceptions to this general rule.") (citations omitted).

This debate informs, but need not determine, the issue before this committee. Invasive, arbitrary border searches that pry into personal communications, family photos, confidential relationships, and business matters are occurring on a regular basis. Congress has the power to limit the scope of suspicionless seizures, thereby strengthening Constitutional protections.

6. **Senator Brownback noted that customs officials at the border could look through hard copies of photographs, and suggested that imposing a reasonable suspicion requirement on laptop searches would convey to people who travel overseas for illegal activities that they should "just put [the photographs] in electronic form and you are more likely to be able to get them through." The implication is that imposing a reasonable suspicion requirement on laptop searches would create a loophole where none existed before.**

   Is Senator Brownback correct? Or are there currently other means by which an American citizen traveling overseas could get photographs across the border in a manner that they would not be subject to suspicionless searches?

Answer: Senator Brownback is not correct because there are numerous means by which American citizens can transport photographs across the border other than on a laptop without being subject to suspicionless searches.

Here are a few examples:

- Photographs can be sent across the border via international mail. Pursuant to regulations promulgated under19 U.S.C. § 1582, border agents cannot open and examine sealed letter class mail without reasonable suspicion that the package contains merchandise or contraband.

- Photographs can be uploaded to private, secure, encrypted, online backup and storage services and then accessed over the Internet from anywhere in the world. There are many companies vying to offer such services, including Box.net, Carbonite, CryptoHeaven, FileWorks, IDrive, Iron Mountain, Mozy, SwissDisk, and many others.

- A user may use an encrypted email system to send copies of photographs to him or herself. Any non-webmail email account can be used for this purpose by using built-in or "plugin" features for email clients such as Microsoft Outlook, Mozilla Thunderbird or Apple's Mail.App. Secure webmail is readily available from providers including Hushmail and Cryptomail. Other software providers offer code that can layer encrypted storage over popular webmail services like Gmail.

- Photographs could be posted in any form (encrypted, steganographically hidden, or even unencrypted) to public websites, news groups, mailing lists or message boards, using anonymizing proxies or even anonymity networks such as Tor to disguise the identity of the users posting and viewing the files in question.

- Photographs can be copied onto a computer located at a data center and connected to the Internet backbone. Different degrees of access and ownership can be purchased at competitive market rates: an account on a shared machine might be $2/month; a private virtual machine might be $5/month, and an entire private computer might be $50/month. With these services, users can deploy the software of their choice for encrypted storage and communication of files. Individuals who retain a permanent residence while traveling can use regular broadband Internet connections in the same way.

Using these methods, a user with contraband photographs would be able to upload the files from one country and download them from another. They could use different computers in each country, or they could use a secure deletion/file shredding program to wipe the files off a laptop before crossing a border, then download them again later.

CONCLUSION

Thank you for the opportunity to respond to these questions.