S. HRG. 110–589

LAPTOP SEARCHES AND OTHER VIOLATIONS OF PRIVACY FACED BY AMERICANS RETURNING FROM OVERSEAS TRAVEL

HEARING

BEFORE THE

SUBCOMMITTEE ON THE CONSTITUTION

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JUNE 25, 2008

Serial No. J–110–103

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

45–091 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ARLEN SPECTER, Pennsylvania
JOSEPH R. BIDEN, JR., Delaware	ORRIN G. HATCH, Utah
HERB KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	JON KYL, Arizona
RUSSELL D. FEINGOLD, Wisconsin	JEFF SESSIONS, Alabama
CHARLES E. SCHUMER, New York	LINDSEY O. GRAHAM, South Carolina
RICHARD J. DURBIN, Illinois	JOHN CORNYN, Texas
BENJAMIN L. CARDIN, Maryland	SAM BROWNBACK, Kansas
SHELDON WHITEHOUSE, Rhode Island	TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
STEPHANIE A. MIDDLETON, *Republican Staff Director*
NICHOLAS A. ROSSI, *Republican Chief Counsel*

SUBCOMMITTEE ON THE CONSTITUTION

RUSSELL D. FEINGOLD, Wisconsin, *Chairman*

EDWARD M. KENNEDY, Massachusetts	SAM BROWNBACK, Kansas
DIANNE FEINSTEIN, California	ARLEN SPECTER, Pennsylvania
RICHARD J. DURBIN, Illinois	LINDSEY O. GRAHAM, South Carolina
BENJAMIN L. CARDIN, Maryland	JOHN CORNYN, Texas

ROBERT F. SCHIFF, *Chief Counsel*
LAUREN B. PETRON, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS AND ANSWERS

SUBMISSIONS FOR THE RECORD

LAPTOP SEARCHES AND OTHER VIOLATIONS OF PRIVACY FACED BY AMERICANS RETURNING FROM OVERSEAS TRAVEL

WEDNESDAY, JUNE 25, 2008

U.S. SENATE,
SUBCOMMITTEE ON THE CONSTITUTION,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 9:06 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Russell D. Feingold, Chairman of the Subcommittee, presiding.

Present: Senators Feingold, Durbin, and Brownback.

OPENING STATEMENT OF HON. RUSSELL D. FEINGOLD, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Chairman FEINGOLD. Welcome to this hearing of the Constitution Subcommittee entitled "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel." We will be hearing this morning from a panel of experts who can help us explore the legal and practical implications of this important issue.

Let me start by making a few opening remarks, then I will recognize the Ranking Member, Senator Brownback, for an opening statement, and then we will turn to our witnesses.

If you asked most Americans whether the Government has the right to look through their luggage for contraband when they are returning from an overseas trip, they would probably tell you yes, the Government has that right. But if you asked them whether the Government has the right to open their laptops, read their documents and e-mails, look at their photographs, and examine the websites they have visited, all without any suspicion of wrongdoing, I think those same Americans would say that the Government has absolutely no right to do that. And if you asked them whether that actually happens, they would say, "Not in the United States of America."

But it is happening. Over the last two years, reports have surfaced that customs agents have been asking U.S. citizens to turn over their cell phones or give them the passwords to their laptops. Travelers have been given a choice between complying with the request or being kept out of their own country. They have been forced to wait for hours while customs agents reviewed and sometimes copied the contents of their electronic devices. In some cases, the

laptops or cell phones were confiscated and returned weeks or even months later, with no explanation.

Now, the Government has an undeniable right and responsibility to protect the security of our borders. The Supreme Court has thus held that no warrant and no suspicion is necessary to conduct "routine searches" at the border. But there is a limit to this so-called "border search exception." The courts have unanimously held that invasive searches of the person, such as strip searches or x-rays, are "non-routine" and require reasonable suspicion. As the Supreme Court has stated, these searches implicate dignity and privacy interests that are not present in routine searches of objects.

So the constitutional question we face today is this: When the Government looks through the contents of your laptop, is that just like looking through the contents of a suitcase, car trunk, or purse? Or does it raise dignity and privacy interests that are more akin to an invasive search of the person, such that some individualized suspicion should be required before the search is conducted?

This administration has argued in court that a laptop can be searched without any suspicion because it is no different from any other "closed container." I find that argument to be disingenuous, to say the least. The search of a suitcase, even one that contains a few letters or documents, is not the same as the search of a laptop containing files upon files of photographs, medical records, financial records, e-mails, letters, journals, and an electronic record of all websites visited. The invasion of privacy represented by a search of a laptop differs by an order of magnitude from that of a suitcase.

Ultimately, though, the question is not how the courts decide to apply the Fourth Amendment in these uncharted waters. I guarantee you this: Neither the drafters of the Fourth Amendment nor the Supreme Court when it crafted the "border search exception" ever dreamed that tens of thousands of Americans would cross the border every day, carrying with them the equivalent of a full library of their most personal information. Ideally, Fourth Amendment jurisprudence would evolve to protect Americans' privacy in this once unfathomable situation. But if the courts cannot offer that protection, then that responsibility falls to Congress. Customs agents must have the ability to conduct even highly intrusive searches when there is reason to suspect criminal or terrorist activity. But suspicionless searches of Americans' laptops and similar devices go too far. Congress should not allow this gross violation of privacy.

Aside from the privacy violation, there is reason for serious concern that these invasive searches are being targeted at Muslim Americans and Americans of Arab or South Asian descent. Many travelers from these backgrounds who have been subject to electronic searches have also been asked about their religious and political views. As we will hear today, travelers have been asked why they chose to convert to Islam, what they think about Jews, and their views of the candidates in the upcoming election. This questioning is deeply disturbing in its own right. It also strongly suggests that border searches are being based, at least in part, on impermissible factors.

The disproportionate targeting of this group of Americans does not mean that other Americans are exempt. The Association of Corporate Travel Executives has surveyed its members, and 7 percent of business travelers who responded to the survey had experienced seizures of their laptops or other electronic equipment. That is an incredible number when you consider how many Americans are required to undertake overseas business travel today and the amount of confidential business information stored on their laptops. As we will be hearing today, the problem is large enough to have a real impact on the way Americans do business.

Americans have tried to find out from the Department of Homeland Security what its specific policies are on searching and seizing electronic equipment at the border. Two nonprofit organizations filed a Freedom of Information Act request in October 2007 to get DHS to turn over its policies. Eight months later, DHS has not complied with that request. My own questions for Secretary of Homeland Security Michael Chertoff on this issue, which I submitted to him in early April after his appearance at an oversight hearing held by the full Judiciary Committee, have not been answered, despite my specific request that they be answered before this hearing.

I asked DHS to send a witness to testify today. DHS responded that its preferred witness was unavailable on the day of the hearing. So I asked DHS to send a different witness, but DHS declined. I felt it was so important to have a DHS witness here that I wrote a letter to Secretary Chertoff last week urging him to reconsider, and that letter will be made part of the hearing record. The Secretary has not responded.

DHS did provide written testimony. That testimony—which, incidentally, was submitted over 30 hours later than the Committee rules require—provides little meaningful detail on the agency's policies and raises more questions than it answers—questions that no one from DHS is here to address.

Needless to say, I am extremely disappointed that the Department of Homeland Security would not make a witness available to answer questions today. Once again, this administration has demonstrated its perverse belief that it is entitled to keep anything and everything secret from the public it serves and their elected representatives, while Americans are not allowed to keep any secrets from their Government. That is exactly backward. In a country founded on principles of liberty and democracy, the personal information of law-abiding Americans is none of the Government's business, but the policies of the Government are very much the business of Congress and the American people.

[The prepared statement of Senator Feingold appears as a submission for the record.]

In any event, I look forward to hearing from the witnesses who did accept my invitation to testify today so we can begin to explore this important issue in more detail. But first let me recognize the Ranking Member, Senator Brownback, for any comments he would like to make.

STATEMENT OF HON. SAM BROWNBACK, A U.S. SENATOR FROM THE STATE OF KANSAS

Senator BROWNBACK. Thank you, Mr. Chairman. Let me pass on my condolences to you and the State of Wisconsin for the flooding that had happened up there. We are going to dealing with it throughout the Midwest. We have had a lot of storms in our part of the country. We have not had quite the level of flooding that you have had, and I know that is something that is concerning all of us and concerning people—

Chairman FEINGOLD. It is rough, yes.

Senator BROWNBACK. Yes, just amazing numbers of things we are going to need to deal with. That is aside from this hearing.

I want to thank the panelists for all being here, and I want to thank you for holding this hearing. I find it a very interesting topic and one I think that is certainly worthy of this Subcommittee to be exploring and to be looking at. I believe it is always informative and challenging to explore the intersection between the needs to safeguard our country against terrorists and criminal threats and the desire and need to protect our citizens' privacy interests. It seems like to me that has been one of the big challenges that we have had to confront as we have served in the U.S. Senate, and we have certainly seen a great amount since 2001 and the September 11th attacks that we have had. These questions only seem to become more and more complicated as technology advances, as travel and communications reflect an ever more globalized society, and as the dangers we face shift from easily identifiable, nation-specific threats to threats from more diffuse terrorist groups and affiliations. These just get to be more and more complicated and difficult, and they need a lot of expertise. That is why I am appreciative of the panel being here and providing your thoughts and your advice.

New technology in some cases, unfortunately, brings with it new ways to misuse technology. The sad fact is that while the vast majority of Americans and visitors to our country use laptop computers and other digital devices for purely legitimate reasons and purposes—business, academic research, personal household management and the like—others use technology for more nefarious purposes. All the cases to address laptop searches at the border, for example, have involved individuals who are transporting child pornography on their computers. We also know that terrorists take advantage of this kind of technology. Mr. Moussaoui, for example, kept information on his laptop computer that, if discovered, might have prevented the September 11th terrorist attacks. That is a sobering thought.

As we examine the question of when and how Government officials may search laptop computers at the border, we face two sets of questions—the first are legal, the second seem to be practical. 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. I think you address that as such. The Fourth Amendment prohibits unreasonable searches and seizures. However, the Supreme Court has long held that border searches are inherently reasonable and, therefore, do not violate the Fourth

Amendment. In the *United States* v. *Ramsey*, the Court examined that 2 months before Congress proposed the Bill of Rights, including the Fourth Amendment, it had enacted a customs statute that gave officials "full power and authority to enter the search" and search "any ship or vessel in which they shall have reason to suspect any goods, wares, or merchandise subject to duty shall be concealed."

The close timing of the customs statute and the Bill of Rights makes it abundantly clear that Congress did not think that border searches and seizures were unreasonable, nor did it intend to require a warrant or probable cause for such searches. The reason for the border search exception seems obvious. Within constitutional limits, a sovereign nation must have the ability to control who and what enters the country. In certain cases, of course, the search will be so intrusive that it must be justified and justifiable by reasonable suspicion. The Supreme Court and the Federal appellate courts have recognized that strip searches, body cavity searches, prolonged detentions, and certain x-ray examinations, so-called non-routine searches are so invasive and embarrassing that they must be based on reasonable suspicions. And I think those are right and those are appropriate to have those limitations on those non-routine searches. Only in cases where they are actually destructive, though, or conducted in a particularly offensive manner do property searches require reasonable suspicion. Otherwise, they are deemed routine searches and are considered reasonable by nature of the very fact that they occur at the border.

The reason that I went through some of the legal analysis very quickly on this—and this does not do any of it just—is it seems here we are having the discussion, OK, what is reasonable and routine, and what is not reasonable and non-routine. And that goes to the question that we are involved in here today.

I hope, Mr. Chairman—and I have a fuller statement to put into the record, but rather than going through that, I would like to get to the panel. I hope we can go through this on a very basis of protecting an individual's right, but also looking at trying to protect the country and getting information that we need to have to be able to protect the country or to get at criminal elements trying to bring material into the country that would be deemed inappropriate, and that we can have a good discussion of what that intersection is in this technology age, in this age of ever increasing globalization, that we can look at this in both a constitutional way and in a way that we can protect the citizenry of the United States.

So I appreciate very much your holding the hearing. I look forward to the witnesses' comments and testimony as we explore this topic.

Chairman FEINGOLD. Thank you, Senator Brownback. I think you have certainly correctly characterized the way we should look at this issue, and I believe your comments were very consistent with my opening remarks as well. We are trying to make sure we get this right.

We will now turn to our panel of witnesses. Will the witnesses please stand to be sworn in? Will you all please raise your right hand to be sworn? Do you swear or affirm that the testimony you

are about to give before the Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. TIEN. I do.

Mr. SALES. I do.

Ms. GURLEY. I do.

Mr. CUNNINGHAM. I do.

Mr. KHERA. I do.

Mr. CARAFANO. I do.

Mr. SWIRE. I do.

Chairman FEINGOLD. Thank you. You may be seated.

I want to welcome you and thank you for being here with us this morning. I will ask that each of you limit your remarks to 5 minutes, as we have a full panel today. Your full written statements will, of course, be included in the record.

We will begin today with Mr. Lee Tien. Mr. Tien is a senior staff attorney at the Electronic Frontier Foundation, a nonprofit organization that works to protect civil liberties and consumer rights in the digital age. Along with the Asian Law Caucus, EFF filed a Freedom of Information Act lawsuit seeking disclosure of DHS policies on border searches and searches of electronic devices. Mr. Tien specializes in free speech and privacy litigation and has written several law review articles on free speech and privacy issues.

Mr. Tien, we are pleased to have you here today, and I appreciate your traveling here from San Francisco to give us your testimony. You may proceed.

STATEMENT OF LEE TIEN, SENIOR STAFF ATTORNEY, ELECTRONIC FRONTIER FOUNDATION, SAN FRANCISCO, CALIFORNIA

Mr. TIEN. Thank you very much. Mr. Chairman, Ranking Member Brownback, the Electronic Frontier Foundation is pleased to discuss an issue of growing importance to Americans' privacy. The problem is simple. The Government claims that it can search any laptop, cell phone, or BlackBerry at the border. It does not matter whether you are a Senator on a fact-finding trip or a tourist on vacation. Your data is fair game.

It is clear that most people regard this as a serious privacy invasion. People keep their lives on these devices: diaries, personal mail, financial records, family photos. Even Secretary Chertoff told this full Committee back in April, and I quote, "There are absolutely privacy concerns."

It is also a free speech problem. Journalists' laptops and cell phones contain drafts of works in progress and records of their sources. The Government should not be able to read this information without a good reason.

And it is a business problem. It is no surprise that a major law firm like Arnold & Porter recently warned its clients about the risks of laptop border searches.

Now, EFF does not dispute that the Fourth Amendment works differently at the border, but differently does not mean not at all. Under the Fourth Amendment, any search must be reasonable. And while a routine border search is reasonable by definition, not all border searches are routine.

There is no bright-line rule here, but the Supreme Court has said that non-routine searches are largely defined by their invasion of a person's dignity and privacy interests. As you have already pointed out, most courts agree that strip searches, x-ray examinations, and body cavity inspections are non-routine.

Our point is that data searches also invade dignity and privacy. Invasiveness is not just physical. Wiretapping invades privacy without any kind of physical intrusion. And because our devices store our thoughts and communications, these searches implicate the First Amendment as well. Fourth Amendment requirements apply with scrupulous exactitude where speech is at issue. In short, searching a laptop, iPhone, or BlackBerry invades dignity and privacy interests and threatens freedom of speech and should require reasonable suspicion, not no suspicion.

I have two more quick points before moving on to a few recommendations. First, the word "search" in this context is slippery. Border agents do not just look at laptops. They copy data and even seize devices. We feel that copying data is a seizure of that data. If the Government has a copy, you have lost your property right to control it. That is especially invasive.

Now, Secretary Chertoff said in April that, as a matter of practice, DHS searches the contents of laptops or cell phones only when there is a reasonable suspicion, and that he believed DHS uses a probable cause standard before seizing a device or retaining copies of its contents. Well, if that is the real policy, there is no reason why these standards cannot be codified in the law.

Second, if border agents can legally search any device at the border, then they can search every device at the border. "Any" really means "every." Without a standard, resources are the only limit on this power, and technology is removing that limit. In February, Microsoft announced the COFEE, which stands for Computer Online Forensic Evidence Extractor. It is a USB thumb drive that contains 150 commands that can dramatically cut the time it takes to gather digital evidence.

In May, the CSI Stick, which stands for Cell Seizure Investigator Stick, was announced. It can capture all data on most models of cell phones or just grab the text messages, phone books and call logs, or multimedia messages.

Now, CBP may already be using such devices. My point is not that they should never do so; rather, it is that agents have great practical power to search and seize personal information. And with great power comes great responsibility. After all, the Fourth Amendment is intended to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals.

Ideally, the courts would modernize border search law. But so can Congress. As Senator Leahy once noted, the law must advance with the technology to ensure the continued vitality of the Fourth Amendment. The same is true here. Congress can protect the privacy of devices that typically contain e-mail and other stored communications and records. Congress can clarify that seizing data and devices requires probable cause. And, finally, Congress can make DHS accountable by requiring border agents to report their

search and seizure activities and informing people of their rights about any seized data or devices.

Thank you for allowing me to testify.

[The prepared statement of Mr. Tien appears as a submission for the record.]

Chairman FEINGOLD. Thanks so much, Mr. Tien.

We will now turn to Professor Nathan Sales. Professor Sales is an Assistant Professor at the George Mason University School of Law, where he teaches national security law and administrative law. Prior to joining the faculty of George Mason, Professor Sales served as Deputy Assistant Secretary for Policy Development at the Department of Homeland Security, and he previously served as Senior Counsel in the Department of Justice Office of Legal Policy.

Professor Sales, thank you for being here today, and you may proceed with your testimony.

STATEMENT OF NATHAN A. SALES, ASSISTANT PROFESSOR OF LAW, GEORGE MASON UNIVERSITY SCHOOL OF LAW, ARLINGTON, VIRGINIA

Mr. SALES. Thank you, Mr. Chairman, and thank you, Mr. Brownback, both of you, for holding this hearing on an important issue.

Before we talk about the law of laptop searches, I would like to spend a few minutes talking about the policy. Why does CBP occasionally search travelers' computers at the border? Well, the answer is because it is an effective way of detecting child pornography and terrorism. Here is the key statistic. There have been 11 Federal decisions testing the ability of CBP to search laptop computers at the border. Every single one of those cases has involved child pornography.

Let me tell you about a man named Stefan Irving. Irving used to be the pediatrician for a school district in New York, but he lost his license and was sent to jail after a 1983 conviction for attempted sexual abuse of a 7-year-old boy. In 1998, after serving his time, he flew back to the United States from vacation in Mexico. Customs officers searched his luggage and found children's books. They also found children's drawings. They also discovered two computer disks. When they looked at the disks, they discovered numerous images of child pornography. It turns out that Irving was in Mexico to visit—and these are the court's words—"a guest house that served as a place where men from the United States could have sexual relations with Mexican boys"; Irving "preferred prepubescent boys, under the age of 11."

Irving is now serving a 21-year sentence. Part of the reason he is behind bars and no longer preying on innocent children is because of a laptop search.

Laptop searches are not just about child exploitation. They are also about terrorism. We have already heard that Zacarias Moussaoui kept a wealth of data on his laptop, including information about crop-dusting aircraft and wind patterns.

In 2006, more recently, a laptop search at Minneapolis-St. Paul helped CBP detect a high-risk traveler. Officers inspected this man's laptop and found video clips of roadside bombs being used

to kill soldiers and destroy vehicles. They also found a video on martyrdom.

So what does the Constitution have to say about laptop searches at the border? Not much, actually. The Fourth Amendment applies differently at the border than it does inside the country. Here is how the Supreme Court puts it: Routine border searches "are not subject to any requirement of reasonable suspicion, probable cause, or warrant."

Let me give you some more statistics. There have been 11 Federal decisions in this area. Seven of the 11 hold that CBP can search laptops with no particularized suspicion whatsoever. Three courts punted. In those cases, the officers had reasonable suspicion to search the laptops, so it was unnecessary to consider the legal issue. Other than a single California district court that was reversed on appeal, no court has held that CBP needs reasonable suspicion. No court has held that probable cause is required. And no court has held that Customs has to get a warrant.

My sense is the Supreme Court is unlikely to disturb this lower court consensus for a simple reason: technological neutrality. The privacy protections we enjoy should not depend on whether we store our information on paper or in the digital world. Officers can search mail, they can search address books, they can search photo albums at the border with no suspicion at all. Why should the rule change when we keep our correspondence, contacts, or pictures on a laptop? The mere fact of computerization should not make a difference to the scope of our privacy rights.

Now, while the Fourth Amendment does not have much to say about laptop searches, it is not the end of the conversation. Policymakers should consider adopting a few safeguards above the constitutional floor. For starters, CBP might usefully shed some light on the standards it uses for picking people for laptop searches. Are they selected randomly? Because of travel history? Because of tips from other Government agencies? What about observations regarding passenger demeanor? More transparency here would help assure people whose laptops are searched that they were picked for legitimate law enforcement reasons and not because of impermissible characteristics such as race or religion.

Also, CBP might adopt standards on what it does with data copied from laptops. If a search does not uncover anything illegal, CBP would be hard pressed to justify keeping files from a passenger's computer. For data that it does keep, CBP should strictly enforce policies that punish employees who access it or disclose it without authorization. Also, CBP should take special care to see that any sensitive business information, such as trade secrets or attorney-client privileged materials, are handled with all appropriate discretion.

Mr. Chairman, thank you again for the opportunity to testify. I would be happy to answer any questions.

[The prepared statement of Mr. Sales appears as a submission for the record.]

Chairman FEINGOLD. Thank you, Professor Sales.

Now we will turn to Susan Gurley. Ms. Gurley is the Executive Director of the Association of Corporate Travel Executives, a nonprofit education and advocacy organization supporting the global

corporate travel industry. Ms. Gurley has been instrumental in the ACTE's development of data privacy, travel security, and corporate social responsibility initiatives. Under Ms. Gurley's leadership, the ACTE has taken an active role in voicing concerns about suspicionless searches and seizures of electronic devices at the border.

Ms. Gurley, thank you for being here, and the floor is yours.

STATEMENT OF SUSAN K. GURLEY, EXECUTIVE DIRECTOR, ASSOCIATION OF CORPORATE TRAVEL EXECUTIVES, ALEXANDRIA, VIRGINIA

Ms. GURLEY. Thank you. Chairman Feingold and Senator Brownback and distinguished members of this Committee, I appreciate this opportunity to present the views of the Association of Corporate Travel Executives, known as ACTE. The seizure of electronic devices from travelers is real, and it is not mere speculation. ACTE represents the safety, security, and financial interests of business travelers, and we represent more than 2,500 members from 82 countries, including the United States. ACTE's members represent over $300 billion in annual business travel expenditures and are among the companies listed in the Fortune 1000.

ACTE's member companies are responsible for over 1 million business travelers and have hundreds of thousands of business travelers on the road at any given time. They routinely cross U.S. borders. All of these U.S. and international business travelers who cross U.S. borders have two things in common: All carry electronic devices, and all are currently subject to the claimed authority of DHS officials to inspect and seize these electronic devices without suspicion or warrant. Thus, ACTE is requesting improved and transparent communications from DHS regarding the policies and safety measures it has in place to protect downloaded data.

We specifically ask that the following actions be taken:

We hope that this Committee requests a Privacy Impact assessment from DHS on the number of seizures of laptops or other electronic devices. The assessment should also ask for the minimum, average, and maximum amount of time that it takes to return the electronic devices to the owner and the reasons for the seizure.

We request that the policies regarding electronic device seizure and data retention policies be published by DHS in the Federal Register and on the agency's home page. These published policies should included at a minimum the following: policies for protecting the integrity of the data; policies for the length of time seized data will be stored and where and how it will be stored; policies for whether the downloaded information will be shared and, if so, with what other U.S. Government and international agencies and under what circumstances; information as to what rights the traveler has to ensure that their electronic device is returned.

I am here to advise you that the seizure, copying, and retention of sensitive business information imposes both a personal and economic hardship on business travelers and their corporations. In today's wired and networked and borderless world, one's office no longer sits within four walls or a cubicle. Rather, one's office consists of a collection of mobile electronic devices. It is common for business travelers to carry their electronic devices that contain

business, financial, and personal information. These devices constitute the office of today. Under the U.S. Constitution, a warrant is needed to search a physical space such as an office. Yet the unanticipated seizure of one's mobile office has been allowed to occur and can immediately deprive an executive or a company of the very data and, most importantly, revenue a business trip was intended to create.

As a businessperson returning to the U.S., you may find yourself effectively locked out of your mobile office indefinitely, and thereby deprived of the resources required to sustain your livelihood. In the case of an independent entrepreneur, a laptop seizure can represent the loss of his or her entire business.

It can be argued that the percentage of seized computers and data is small in comparison to the total number of travelers crossing the border. But we simply do not know. Due to DHS' lack of transparency, the actual number of seizures, the extent of data downloading, and potential data breach are not known. Here is what we do know: ACTE surveyed its members in February 2008 on this issue. Seven percent reported that they had been subject to the seizure of a laptop or other electronic device. The survey also revealed that 81 percent of survey respondents were unaware that the informational electronic devices could be copied and held indefinitely. Even though the total number of business travelers subject to these searches and seizures can only be estimated, what is certain is the severe economic and behavioral impact that can follow when a laptop is seized. Fifty percent of the respondents to ACTE's 2008 survey indicated that having a laptop seizure could damage a traveler's professional standing within a company. The seizure of data or computers carrying business proprietary information has and will force companies to implement new and expensive internal travel policies.

In fact, this is already happening. Costly and time-consuming travel measures that companies are mandating include having their business travelers send data to themselves via web-accessible e-mail, encrypting files, or using secure USB drives. In addition, companies are purchasing additional computers that are scrubbed of any prior e-mails so that they can be used by business travelers on their trips.

All of these measures and business behavior changes cost time and money. In today's economy, American businesses do not need additional and unnecessary financial burdens placed upon them.

Thank you very much.

[The prepared statement of Ms. Gurley appears as a submission for the record.]

Chairman FEINGOLD. Thank you, Ms. Gurley. I will now turn to Mr. Larry Cunningham. Mr. Cunningham is an Assistant District Attorney in Bronx County in New York City and in short order will be starting work as an Assistant Professor of Legal Writing at St. John's University School of Law. He has also taught law courses at Brooklyn Law School, Texas Wesleyan University School of Law, Stetson University College of Law, and Texas Tech University School of Law.

Mr. Cunningham, welcome to you as well, and you may proceed.

STATEMENT OF LARRY CUNNINGHAM, ASSISTANT DISTRICT ATTORNEY, BRONX COUNTY; ASSISTANT PROFESSOR OF LEGAL WRITING, ST. JOHN'S UNIVERSITY SCHOOL OF LAW, QUEENS, NEW YORK

Mr. CUNNINGHAM. Thank you, Mr. Chairman, and I would also like to extend my appreciation to you for holding this hearing on this very important topic.

I taught the law of search and seizure as both a full-time and adjunct professor. I have also conducted research and written in the area of border searches, and this is what I found.

Historically, the Government has had broad authority to conduct searches at the international border without suspicion and without the need to obtain warrants. Case law speaks of the sovereign having an inherent right to protect the country from the importation of illegal or dangerous items. The Supreme Court has also recognized that persons who cross the border have a low expectation of privacy, in part because even if the United States adopted a relaxed border search policy, travelers would still be subjected to search by the countries that they would be traveling to or from.

The Supreme Court has required reasonable suspicion only when an invasive search of the human body is contemplated. The rationale for this higher standard is concern for the dignity of the person, not just privacy. I have uncovered no appellate court decision that has extended this same protection to laptop computers.

Without doubt, anyone whose property has been searched, whether it is a laptop or a briefcase, will feel that his or her privacy has been violated. However, the Constitution recognizes that some governmental invasions of privacy are permissible. After all, the Fourth Amendment does not prohibit searches, only unreasonable ones.

There is also no doubt that many people do keep very personal information on their laptop computers, but the same can be said for travelers who keep their checkbooks, medications, photographs, political literature, love letters, or personal diaries in their briefcases or luggage. No one likes the idea of the Government seeing these things, yet absent a drastic change in the law, each of these tangible, non-electronic items can be seen and examined by customs without reasonable suspicion.

So the question boils down to this: Is there something different about laptop computers that warrants disparate treatment from briefcases, suit pockets, and purses? Some would argue that there is, because laptops are readily capable of storing large amounts of information and that in some cases even deleted items can be undeleted and read. However, the Fourth Circuit in *United States* v. *Ickes* pointed out that in-depth searches are likely to be few and far between because of the lack of resources and time. In fact, the case law on this subject demonstrates that the typical laptop search is quite cursory, with travelers simply being asked to quickly open and power on their computers for a quick visual inspection. Full-scale searches and the un-deleting of files are reserved for situations in which the initial observation has aroused an agent's reasonable suspicion.

There are significant societal interests at stake here. Each of the cases I have found, as Professor Sales mentioned, have involved de-

fendants attempting to bring child pornography into the country. Congress itself has recognized the importance of catching and punishing this criminal behavior by providing steep penalties for the importation, distribution, and possession of child pornography. Moreover, as the Fourth Circuit recognized in Ickes, without a robust, random border search policy, terrorist or other international criminals could use laptops as a means to smuggle messages and plans into the country for distribution to cells and allies. Such a means of communication might prove more attractive than traditional phone or Internet communications because of the possibility of surveillance.

It would seem prudent, however, for the administration to require these searches to be conducted by trained personnel, under supervision, and away from public view, and to disclose records of searches which they acknowledge in a Supreme Court case that they keep to not only the DHS Inspector General but also to this body in closed session to ensure that searches are not being conducted in a racially discriminatory manner or for other improper reasons.

Finally, nothing in the Constitution, at least in my view, would permit the Government to seize a laptop or copy or otherwise retain its contents without some suspicion that it contained evidence of a crime. Such a seizure would be a violation, in my view, not just of the right to privacy but also of the owner's property interest in the computer.

Mr. Chairman, I would be glad to answer any questions that you have.

[The prepared statement of Mr. Cunningham appears as a submission for the record.]

Chairman FEINGOLD. Thank you, Mr. Cunningham.

We will now turn to Farhana Khera. Ms. Khera is the President and Executive Director of Muslim Advocates in San Francisco, California. Muslim Advocates is a national legal advocacy and educational organization dedicated to promoting freedom, justice, and equality for all, regardless of faith, and serving as a legal resource to promote the full and meaningful participation of Muslims in American civil life. Prior to her work with Muslim Advocates, I was lucky enough to have Ms. Khera on my Constitution Subcommittee staff here in the Senate. Ms. Khera and I worked together for 6 years, and I am indebted to her for her work and advocacy on issues ranging from the PATRIOT Act to racial profiling to women's rights. The record should reflect that she is a wonderful person and was a wonderful staff member. I am pleased to have her back in the Senate, if only for the morning.

Ms. Khera, you may proceed.

STATEMENT OF FARHANA Y. KHERA, PRESIDENT AND EXECUTIVE DIRECTOR, MUSLIM ADVOCATES, SAN FRANCISCO, CALIFORNIA

Ms. KHERA. Thank you very much, Mr. Chairman, especially for those very kind, kind words. I do not think I would have imagined myself being on this side of the dais during those 6 years.

Mr. Chairman, Senator Brownback, good morning. On behalf of Muslim Advocates, I am pleased to share with you the experiences

of Muslim, Arab, and South Asian Americans returning home from international travel.

The Department of Homeland Security and Customs and Border Patrol have an important duty to protect our borders. The American people, including Muslim Americans, rightfully expect these agencies to protect us from those who would seek to enter to do us harm. But at the same time, we expect our Nation's border policy to be sound. It should be rational, fair, and effective.

Complaints from Americans traveling overseas received by Muslim Advocates and other civil rights groups, however, suggest otherwise. These Americans report that at airports and border crossings, after they have verified their identity and described the purpose of their travel, they have been subjected to more intensive scrutiny, all without any reasonable suspicion that they are engaging in criminal activity. These experiences involve not only searches and seizures of laptops, cell phones, and digital cameras, but perhaps even more troubling, questions about First Amendment-protected matters.

Mr. Chairman, my written testimony sets forth a number of these complaints, but this morning I would like to share with you two of them.

The first is that of an executive vice president of a major high-tech firm in the greater Seattle area. He is a husband, father of three, and a business leader who has helped drive innovation in our country. He has also been a community leader, having established a mosque and spearheaded interfaith activities with Christian and Jewish communities. He has testified before Congress on IT issues, was recognized by the Interfaith Alliance, and is proud to call America home.

He travels frequently due to the demands of working for a global company. Since early 2007, on at least eight occasions, he has been subjected to invasive and intensive questioning, searches, and seizures upon his return home from travel to various countries, including Japan, Canada, Turkey, the U.K., and Europe.

CBP agents have interrogated him about the names, birth dates, and addresses of family members living abroad and in the U.S., which mosque he attends, and his activities on behalf of a lawful Muslim charitable organization he helped establish near his home. CBP agents have also searched his cell phone, made copies of various documents on several occasions, and extensively searched his belongings, as well as those of family members traveling with him.

Mr. Chairman, the second story is that of a young corporate lawyer, a graduate of Georgetown University Law Center and currently practicing with a prominent law firm on the west coast. She in many ways embodies the American dream. The child of immigrants from Pakistan, she grew up in the northern central valley of California. She worked hard, went to top schools, and has established herself with a stable career, making her family proud. This spring, she took a trip to Pakistan to visit her relatives. On her return, which was a 20-plus-hour trip via East Asia to San Francisco, she was exhausted from the long travel and frustrated after learning that the airline had lost one of her bags. After she presented her passport and verified her identity, she, nevertheless, was pulled aside and her remaining bags were searched. The CBP

agent took her digital camera, viewed its images, and asked her to identify the people photographed. Her camera included photos of her mother during her travel overseas, as well as photos taken of her family and friends while she was in the U.S. The CBP agent also saw a book in her bag on one of the Presidential candidates and then proceeded to ask her her views of the candidates in this year's race.

We have reason to believe that these stories are not isolated but, rather, suggest a troubling pattern of targeting Americans who are Muslim or of Arab or South Asian descent. If so, it would be wrong and a violation of the equal protection guarantees of our Constitution.

These experiences also suggest that CBP's power at the border is overly broad and its practice and policies ineffective. I think we can all agree that neither the corporate vice president nor the young lawyer pose a threat to our security nor engaged in wrongdoing.

So why were these Americans stopped? How is CBP power being used? These and other questions must be answered. DHS and CBP have a critical responsibility to protect our Nation's borders. At the same time, these agencies, which have been granted enormous power by the American people, have an obligation to wield that power consistent with the rights and protections guaranteed by the Constitution to all Americans, regardless of faith, ethnicity, or race. And Congress must ensure that they do so.

I refer the Subcommittee to my written testimony for specific recommendations for steps Congress can take.

Mr. Chairman, thank you for the opportunity to present the views of Muslim Advocates and for holding this hearing. I look forward to your questions.

[The prepared statement of Ms. Khera appears as a submission for the record.]

Chairman FEINGOLD. Thanks so much, Ms. Khera.

Next up is James Carafano. Mr. Carafano is the Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies, and Senior Research Fellow at the Douglas and Sarah Allison Center for Foreign Policy Studies, both at the Heritage Foundation. He is an expert in defense affairs, military operations and strategy, and homeland security. Mr. Carafano is a graduate of West Point, and he also holds a master's degree and doctorate from Georgetown University and a master's degree in strategy from the U.S. Army War College.

Mr. Carafano, thank you for being here today to share your testimony. You may proceed.

STATEMENT OF JAMES JAY CARAFANO, ASSISTANT DIRECTOR, KATHRYN AND SHELBY CULLOM DAVIS INSTITUTE FOR INTERNATIONAL STUDIES, AND SENIOR RESEARCH FELLOW, DOUGLAS AND SARAH ALLISON CENTER FOR FOREIGN POLICY STUDIES, THE HERITAGE FOUNDATION, WASHINGTON, D.C.

Mr. CARAFANO. Thank you, Mr. Chairman. I want to offer five principles for congressional action. These are based on my years of research and experience looking at border security issues.

Just an observation as a preamble. The mission of Homeland Security and, indeed, the mission of Government is to enable Americans to live their lives in freedom, safety, and prosperity and to implement policies that serve all three of those goals equally well. That is nowhere more important than the issues of border security.

One of my great frustrations is that we myopically often talk about border security and just focus on the border when, in reality, the way you make a border secure is addressing any criminal or malicious or terrorist activities. It is really thinking about the spectrum of terrorist travel or malicious activity from its origin to its point of destination in the United States, and not myopically focused just at the border. However, border security is important, and nowhere is it more important than at our ports of entry and exit. We have enormous data on known terrorist travel, including the 9/11 Commission report. Overwhelmingly what we know is known terrorists travel mostly through established points of entry and exit. And we know that a wide variety of criminal and malicious activity also enter and exit our legal points of entry and exit. So getting it right at the ports of entry and exit is nowhere more important.

I think there are number of vital issues here for the Congress to address. Actually, the legal issues would not be highest on my list. Much more important, I think, are infrastructure issues and creating a border infrastructure that we need both to do inspections expeditiously and effectively and to reduce transaction times in our border which are increasing and are increasing the cost of doing business in the United States.

Border searches are a vital part of the port of entry and exit. I do not think that is questions. We all know the most famous case of all, which was the millennium bomber, where a border officer asking some very, very innocent questions—including "Where are you going?" and "Where are you staying?"—was able to identify a high-risk traveler, and an inspection later showed that he was carrying explosives and was planning to blow up a target in Los Angeles. So getting it right is incredibly important.

For me, the efficacy of border searches will lie less in the issues of narrow legal opinions and much more on the issues of focusing on the critical technology and human capital programs that the Department has to implement so it can do these border searches in an effective and reasonable and secure manner. So I would offer five guidelines for the Congress as it thinks through where it is headed on this.

First and most importantly, from a security standpoint, it would be a grave mistake and an error to create any technology as a sanctuary, where someone had a sanctuary in terms of bringing materials into the United States, and anything that impeded the ability to conduct reasonable and routine searches of any technology or emerging technology would be an enormous mistake.

Second, the border agents need to retain broad authority in how they implement their powers. They have limited time and limited information to make their inspections. Obviously, human capital programs and added technology will improve their efficiency. But at the end of the day, we do rely on the men and women standing

at the border to get it right, and we have to give them the broad authority that they need to do their job.

And, third—and this I think is important; I do not think anybody on the panel has mentioned it—we need to really make sure that we do not force the Department to disclose a level of information that would allow malicious actors, whether they are criminals or terrorists, to identify specific patterns of inspection and behavior that would allow them to figure out how to bypass security inspections at the border. So we do, from an operational security standpoint, have to be careful about how much information we publicly disclose, although I think the issue of transparency is vitally important. We should disclose as much as possible, and certainly Congress should be informed on these critical issues.

Fourth, any process of inspecting at the border has to be risk-based. Any inspections that are merely based on whim or any kind of racial profiling are wrong not just from a legal standpoint, but they are even more wrong from an efficiency standpoint. You have scarce time and scarce resources at the border. Wasting them on people who are not high-risk travelers is simply unconscionable behavior. And all inspections, all reasonable searches, should be based on risk-based assessments.

My last point is that there should be, obviously, a requirement that as DHS deals with any kind of data they inspect at the border, that they deal with it in a responsible and professional manner.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Carafano appears as a submission for the record.]

Chairman FEINGOLD. Thank you, Mr. Carafano.

And, finally, we turn to Professor Peter Swire. Professor Swire is a professor at the Moritz College of Law at the Ohio State University and a Senior Fellow at the Center for American Progress Action Fund. He is an expert in the fields of privacy law and computer security. From 1999 to 2001, he served as Chief Counsel for Privacy in the U.S. Office of Management and Budget. In that role, he was responsible for coordinating administration policy on public and private sector uses of personal information.

Professor Swire, thank you for coming, and you may proceed.

STATEMENT OF PETER P. SWIRE, PROFESSOR, MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY, AND SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS, WASHINGTON, D.C.

Mr. SWIRE. Thank you, Mr. Chairman.

There is no dispute today that with the right factual basis, the Government can search laptops. The focus of the hearing is when they do not have that kind of suspicion and basis, what should the policy and the law be, and that is what we will focus on.

I agree with many of the concerns already expressed today by you, Mr. Chairman, and by other witnesses. The focus of my testimony is on comparisons to the encryption policy battles we had in the 1990s and that I worked on when I was in the White House. At that point, we treated things very differently in encryption when across the border, and we tried to use the border for a while as Government policy as an excuse to search computing in very intru-

sive ways. That policy was eventually rolled back, and I am going to list eight comparisons today between the encryption battles then and laptop border searches today.

The first one is that traditional legal arguments apply badly to new facts about computing. In the encryption policy area, there is a legal tradition that wiretap orders were going to be effective, and so the Government wanted wiretap orders to be effective even when there was encryption, so we needed to get all the encryption keys.

Today, the Government in the laptop area is saying it is the same old border searches we have always seen for 200 years; there is nothing to see here and move on. But I think there is something to see here, and that is why we have the hearing today. A laptop contains all of the books printed in human history up until sometime into the late 20th century, and the idea that we are just going to trust the Government with this amazing ability to copy all this data I think is a concern and something different.

The second comparison is that the Government forces disclosure of encryption keys. For people who do not spend their time focusing on encryption, which is most normal people, I will give a quote from the founder of EFF, who said, "You can have my encryption algorithm, I thought to myself, when you pry my cold dead fingers from its private key." Getting people's encryption keys at the border is a big deal. It led to a big fuss once before.

Number three is that these kinds of searches are a severe violation of computer security best practices. My testimony explains this in some detail, but the basic rule in computer security is do not let strangers into your computer. You can get infected. You can have malware put on it. You can never entrust that platform again. It violates best industry practice. It violates all the training we are doing in our security infrastructure if we have routine searches of business computers. It should not happen.

Fourth, the U.S. policy can create bad precedents that totalitarian and other regimes can follow. I invite you here to think about if China or other countries going forward make their customs something like this: step one, go through customs; step two, make a copy of your hard drive; step three, we will see you next time. And if that applies to Senators and their staffs when they go on foreign missions, you are not going to want to have that as policy. If the U.S. does border searches all the time and it becomes increasingly easy with technology to make these copies, then we have gotten on the wrong side of the issue. It is hard for us to complain when other countries intrude into our privacy.

The fifth comparison is severe harm to personal privacy, free speech, and business secrets. Other witnesses and my written testimony talk about these invasions of privacy, the problems for free speech and the rest.

A sixth comparison with the encryption battles of the 1990s is the disadvantages to the U.S. economy. That was a major strike against the encryption policy because we were helping foreign competitors. When it comes to foreign conferences that will not want to come to the United States, when it comes to the idea of whether the U.S. is open for tourists and for business to visit without feel-

ing deeply intruded, I think we have to think about the effect on the U.S. economy of intrusive searches at the border.

A seventh comparison to the encryption battles is the political coalition that developed of civil liberties groups and business. We see that today. It is a similar line-up to what we had 10 years ago where we have EFF, we have the Muslim Advocates, we have business groups complaining here. And for someone such as I who spent a lot of time with the tech community, I think this issue may be a much hotter thing than people have realized. It may mobilize the reserve army of outraged techies. And if that happens, we are going to see a lot of yelling and screaming and a lot of concerns from corporate and other security experts. This is, again, I think a big deal.

The eighth and final comparison I would make between encryption in the 1990s is the technical futility of current U.S. policy. In crypto, we eventually saw that there were work-arounds to the U.S. policy. Those work-arounds already exist and are easily found on the Internet today. I cite in my testimony articles on the Internet that tell you how to keep your data secret from customs when you go through the border. Any moderately smart terrorist can find these articles if they just read the hearing transcript for today, for instance, and they will be able to get through the border. And also if they are willing to lie, they can get standard software today where they can double encrypt their laptops so the customs people cannot find it.

So for these eight comparisons, we see that it is bad policy and ultimately futile to have this. It invades computer security and privacy and free speech and business secrets and sends the wrong signal to the rest of the world, and I think we should change the policy.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Swire appears as a submission for the record.]

Chairman FEINGOLD. Thank you so much, Professor, and thanks to all of you for your excellent testimony.

I will start a round of questioning. Senator Brownback had to go to something else, but he is going to try to come back to ask questions as well. So I am going to start going through my questions, but obviously, if and when he comes back, we will turn to him and any other Senator who wants to ask questions.

Before we go to the questions, though, there have been some very informative news reports on this subject recently, including a February 7, 2008, article in the Washington Post and an article posted yesterday on the U.S. News & World Report website. Without objection, these will be made part of the record.

Also, Senator Leahy, the Chairman of the full Committee, has a statement he would like to put in the record, so without objection, I will do that as well.

I will start the first 7-minute round. Professor Swire, some of the witnesses here have testified that we must allow suspicionless searches of U.S. citizens' laptops at the border because laptops can contain evidence of serious crime or even terrorism. Obviously, I do not dispute that laptops can contain such information. But, of course, that very same evidence can exist on laptops located inside

U.S. citizens' homes. And yet even if there were no constitutional barrier whatsoever to police officers walking into your house to conduct suspicionless laptop searches, I think we would all agree that such searches should not be permitted.

As a policy matter, do you believe the liberty, privacy, and economic interests at stake in these border searches outweigh any security benefit to be gained by conducting them?

Mr. SWIRE. Yes, I do, Senator. Thank you. I think when people cross the border these days using the Internet, they can use strong encryption. We have that written into law now. When people are at home, they can use strong protections against these kinds of invasion. The idea that you are at the border and you have to reveal your passwords and encryption keys is something that is quite remarkable. It is very intrusive. It is bad for privacy and security. And we do not—a couple of the witnesses in their written testimony talked about the principle of technology neutrality, that we should not treat laptops different from other things. Technology neutrality is we can cross the border today using strong encryption, using the Internet. And I think technology neutrality says that same computing should cross the border in laptops. So we as a matter of policy should have much stricter limits than we do currently in this area.

Chairman FEINGOLD. Ms. Gurley, one argument in support of allowing suspicionless laptop searches is that customs agents have always been free to search the contents of briefcases, which also carry confidential business information such as trade secrets or attorney-client communications. But there is a big difference between rifling through documents in a briefcase to look for weapons or contraband and picking up the documents and reading them. I would imagine that if customs agents had been reading business documents, we would have heard about a long ago.

Is that right? Or has it always been a normal part of business travel for customs agents to read and even copy the documents in travelers' briefcases?

Ms. GURLEY. It is our understanding that customs would look for contraband, and they would only copy the information that had a nexus with the contraband or the actual potential crime. The difference here is that they basically copy everything, so the vast amounts of information that are being copied are beyond the actual potential crime. So it is not just contraband. It is anything, including the fact that if you were a businessperson and you were carrying documents across the border, those were physical documents. If I am carrying as a businessperson my computer over, I also have erased documents. They can get to that as well. If I have one or two, I drafted something, I have deleted it, customs can, in fact, copy that as well and find it. In the olden days, if I did not bring it, they could not find it.

But the big issue for the business travel community is let's say you are not a pornographer, let's say you are not a terrorist. Let's say you are not engaged in any criminal activity. You are a businessperson. You are people like us doing their regular business, and your information is seized. The data is downloaded. And it turns out there is nothing going on. Why can't the U.S. Government tell us how long they are going to retain the information? Are

they going to destroy the information? What are the doing with that information? That lack of information causes incredible anxiety to the business community, and putting all the constitutional law issues aside, which are critical, the issue is we should have a transparent Government. We find that there is no criminal activity. Why can that information not be returned?

Chairman FEINGOLD. Let me just pursue the briefcase question so I can get a sense of what the current practices are. Were you suggesting that the only thing that would trigger the reading or copying of a document would be the presence of contraband? Or let's say somebody was stupid enough to write down in a letter that they would like to buy some drugs. Would customs agents read that letter, apart from the contraband being in there, and make a copy?

Ms. GURLEY. I would assume they would make a copy of that, and that makes eminent sense. If you find a letter saying I am a drug dealer—

Chairman FEINGOLD. Apart from there being contraband present within the briefcase.

Ms. GURLEY. Right. But now they would go through every piece of information, including your love letters, including your bank—so there is a big difference in how information is disseminated and brought across borders now than even 15, 20 years ago.

Chairman FEINGOLD. Fair enough. An excellent answer.

Mr. Tien, I have a related question for you. A few of today's witnesses have claimed that under existing case law, specifically *United States* v. *Ramsey*, customs agents are allowed, without any reasonable suspicion, to read the contents of paper documents that U.S. citizens carry or send across the border. But as you know, the Supreme Court in *Ramsey* held only that customs agents could open international mail—in that case, to see if it contained heroin. Indeed, the primary reason the Court rejected the defendant's First Amendment challenge is that a Federal statute prohibited customs agents from reading international mail without a warrant.

Are you aware of any case in which the Supreme Court has held that customs agents can read the contents of travelers' personal documents without any reasonable suspicion?

Mr. TIEN. Well, Senator, you are absolutely right about the way that *Ramsey* does that, and I am not aware of any cases that have specifically authorized that kind of reading. This is one of those situations where the Supreme Court case very, very clearly says we do not need to decide this First Amendment issue because we already have congressional and regulatory protections for the privacy of people's mail. The current law may be slightly different, and one of the things that I wanted to point out, especially in conjunction with Ms. Gurley's testimony about transparency, is that when we have asked CBP for documents about how they handle the looking at or the photocopying of documents, we get back from CBP redacted, blacked-out sections about their policies and practices with respect to documents. So it is very unclear.

Chairman FEINGOLD. Thank you, sir.

Ms. Khera, the conduct you have described on the part of customs agents is quite shocking. I think most people here would agree that customs agents should not be asking travelers why they

converted to Islam, for example. I suspect if a DHS official were here, he or she would say that DHS does not condone these questions, that these are isolated cases of customs agents behaving badly. But, of course, the only way to ensure a certain level of conduct is to require it, and to punish any violations of that requirement.

To your knowledge, are there any DHS regulations or any Federal laws that specifically prohibit customs agents from engaging in the kind of questioning identified in your testimony?

Ms. KHERA. Mr. Chairman, we are not aware of any specific regulations that govern CBP in this area. We believe that CBP is instead relying on age-old statutes as well as we have reason to believe that they are relying on internal policy guidance. But the problem is that that internal policy guidance is not public. My colleagues, the Electronic Frontier Foundation and the Asian Law Caucus, have actually sought to get copies of policy guidance, directives, potential training materials that are given to CBP agents. And CBP has not been forthcoming about that material. I think as we have been discuss this morning, in order to for Congress and the American people to understand how the power, the immense broad power of CBP is being used at the border, we do need that information, and I think Congress should be rightfully seeking that information.

Chairman FEINGOLD. Thank you.

As promised, Senator Brownback has returned to do a round of questions, and I also want to welcome Senator Durbin, who has joined us.

Senator BROWNBACK. Thanks, Mr. Chairman. I want to apologize to the panel and to the Chairman. I had another hearing that I was Ranking Member on. They did not both consult me on the time of this. I do not know why I do not get a little more respect around here. Maybe I should take that as a notice.

I want to ask, if I could, it seems like in both the Chairman's and my opening statements, we agreed kind of on the premise, and then we both have questions then on the practicality and the implementation of this, is what the Fourth Amendment applies to as far as at the border, the rights of the country to be able to protect itself, and seeking information, and then this area that the court has tried to figure out is where does the search become so invasive that it is subject to a higher-level standard of review. That is the rub point here.

Professor Sales, I wish I could have caught the rest of your testimony. I apologize. But I appreciated your trying to weave through that. How is it that you look at the issue of a search of a laptop at the border? Is that something that needs to have a heightened level of review or not, as you would look and reading the Fourth Amendment decisions that have come down? I take it from what your testimony was that the majority of courts are saying it does not require that.

Mr. SALES. Yes, Senator, that is right. My sense is that courts have held—and the Supreme Court, if presented with the question, would hold—that reasonable suspicion is not required to justify a laptop search at the border. There is no question, Senator, that laptops are different from a suitcase. A laptop is a container, like

a suitcase is, but a laptop is capable of containing vast amounts of data. An 80-gigabyte hard drive can store, I think, the equivalent of tens of millions of printed pages. So laptops are different.

The question, however, is whether laptops are different in a constitutionally significant respect, and I think the answer to that question is probably no. I think Customs already has broad authority under the Supreme Court's border search precedents to search property, even property that contains extremely sensitive information. I would actually commend to you a Texas district court decision that was released just last week. This opinion discusses the sorts of property that are subject to border searches, suspicionless border searches: people's wallets, purses, locked glove boxes, locked containers or luggage, State and Federal identification cards, Social Security cards, medicines and medical records, names and addresses of family and associates, day planners with itineraries and travel documents, credit cards, checkbooks, registries. The list that the court provided goes on and on.

Senator BROWNBACK. When I have been on the border, I have seen x-ray machines that sat there apparently for some routine searches of big trucks in some settings like that. Those are used even as, I guess, an invasive type of device.

But I have to say as well, too, you know, I do not like the idea of coming across with my BlackBerry and somebody saying, OK, I want to look through your whole BlackBerry, because I have got a lot of things in it. I do not know what all is on there in some cases, and I do not want people looking at that randomly. Do I waive that right in coming across the border?

Mr. SALES. Well, Senator, understandably, people treat the personal data that they store on their electronic devices with great sensitivity, and they regard it as very important. But the Supreme Court has held that the expectation of privacy at the border is different than the expectation of privacy within the country. So while we would rightly condemn suspicionless or especially warrantless searches of your BlackBerry or your laptop on the streets of Washington, D.C., the analysis has to change a little bit at the border. And the Supreme Court has held that the criterion of reasonableness at the border is the fact that it is the border. In other words, a border search is reasonable under the terms of the Fourth Amendment because of the simple fact that it occurs at the border.

Senator BROWNBACK. Mr. Tien, I do not know if you note in your testimony—somebody did—that you can search—if you have got a bunch of photographs with you and you are coming through the border, the border agents can search and look through those photographs. Is that correct? And that is deemed routine. Is that correct?

Mr. TIEN. Under current law, yes.

Senator BROWNBACK. But if we have a digital camera, I take it from what you are putting forward, you are saying, Well, I do not think that is reasonable to do a digital camera.

What is the difference between looking at those two at the border?

Mr. TIEN. What we have been talking about is a general category of electronic devices that range from a laptop and your BlackBerry to a digital camera. And our feeling is that for all of these, you have a number of differences between the sort of non-electronic

version and the electronic version, and probably the most important—

Senator BROWNBACK. Which is? What is the difference?

Mr. TIEN. There is a quantity difference. There is a quality difference. And I think sort of to extend the point that Professor Sales made, there is a scope of search difference. The quantity difference is simply that you can have way, way more information: an 80-gigabyte drive is just an unbelievable amount of information.

Senator BROWNBACK. I am getting short on time here. I just have some question about whether quantity raises your level of expectation of privacy at the border and your other—but let me also pursue this with you if I could. If we were to as a Congress say we want to tighten up this authority for what the border search could do, wouldn't we be conveying to people that travel overseas for illegal activities, wouldn't we be conveying to them just put it in an electronic form and you are more likely to be able to get through than if you had something in a physical form of a physical picture? Isn't that the tactic then that people that would seek to break these laws and do these crimes take?

Mr. TIEN. I do not really think that is a major problem when you consider a couple of things.

First, existing law protects international mail. That is actually the law that the Supreme Court pointed to in *United States* v. *Ramsey*, where they noted that you need reasonable suspicion under statute to open up an envelope and would need a warrant based on probable cause in order to read the correspondence in the envelope. That is why the Supreme Court in *U.S.* v. *Ramsey* did not touch the First Amendment issue. So we have already got laws on the books, for instance, that establish privacy for correspondence.

Second, when we do this electronically, we have the protections under the Wiretap Act that control whether or not those kinds of communications can be searched.

So I do not really see that—from a transparency perspective that we are really telling folks anything more about the privacy interests or about the possibility of evading detection through protecting laptops and BlackBerries and iPhones any differently.

I also wanted to respond to one of your earlier points, Senator, about quantity. I was not saying that quantity is the only reason to differentiate digital devices. There is also the fact that the nature and the question of information on those devices is, it seems to me, much more personal because of the nature of the way that these devices have really embedded themselves into both our personal lives and our work lives. And what that ends up meaning is that your devices are like carrying a giant autobiography of the person in a way that is very different from most physical conveyances, and that creates what I call a scope of search problem.

The purpose of or the function of a legal standard like reasonable suspicion or probable cause is not merely to establish the threshold reason for being able to perform a search. It also establishes the standard for the scope. How far can the search go? If you have probable cause to search something, then that also entails how much of something you can search. Because once you go past the amount that the suspicion or the cause, then you have gone too far.

The Fourth Amendment was intended to prevent general searches and general warrants, things without particularity. And so the idea of having—

Senator BROWNBACK. I think I got the point here from you. I just do really question if we are not conveying a signal to people then that here is the way you get these in and you have a heightened protection at the border rather than another. And I still, though, have real trouble with the idea of people do bring these devices, I use them and bring them across the border because I hope to be able to use them when I am traveling. So I do think we have a real question to wrestle with.

Thanks, Chairman.

Chairman FEINGOLD. First let me compliment the Ranking Member for the balance and quality of his questions, and I just want to review the question that was asked of Professor Sales.

Senator Brownback specifically said he did not like the idea of his BlackBerry being unloaded at the border, and he asked specifically if he waived his right to do that. You gave a scholarly answer, and I heard every word of it. But the answer can only be, based on your words, yes, Senator Brownback has waived his rights.

Mr. SALES. Senator, I would not take credit for that myself. I would say those are the Supreme Court's words.

Chairman FEINGOLD. Fine, but I just want everyone to know that is the whole core of why we are having this hearing. Senator Brownback's rights to privacy of his BlackBerry are waived completely at the border, according to your interpretation of the Supreme Court. And I think that is something we have to examine.

Mr. SALES. If I could, Senator?

Chairman FEINGOLD. Yes, sir.

Mr. SALES. Thank you, Mr. Chairman. There is no question that when crossing the border, a U.S. citizen retains his Fourth Amendment right against unreasonable searches and seizures. The Fourth Amendment applies at the border. The border is not a Fourth Amendment-free zone.

The question then becomes what kind of search counts as reasonable, and the Supreme Court has held for a number of decades that a routine border search can take place with no reasonable suspicion whatsoever.

So the answer to your question, I believe, is the Supreme Court has said "yes, but."

Chairman FEINGOLD. Yes, but the "but" does not you any good because it is a "routine" search so everything is open. Now I am going to turn to Senator Durbin for his round.

Senator DURBIN. Thank you, Mr. Chairman, for this hearing.

About 10 years ago, the NBC television station in Chicago received a complaint from a woman who said she was traveling routinely through Chicago O'Hare, was stopped and strip searched, and she thought it was outrageous. She was African-American. The story ran on the air, and as a result of that story, a number of other African-American women who had gone through the same experience called the station. The woman who handled the story decided to make a plea that all of the African-American women who had been strip searched at Chicago O'Hare should contact the station, and it ended up with I think close to 20 when it was over.

It turned out that the U.S. Customs Service had established a practice at Chicago O'Hare that if you were an African-American coming from certain countries in the Caribbean, that they were going to stop more of them, detain them, and search them. Clearly, this was a case of profiling, and the complaint was made and an investigation initiated. The GAO investigation that I requested found there was a clear pattern of profiling against African-American women. You can understand the personal outrage of these women who were traveling, under innocent circumstances, who were being singled out.

As a result, Ray Kelly, who was then head of the Customs Service, announced that that would end, and I commended him for doing the right thing.

Now I am hearing complaints from particularly my Pakistani-American friends, but others, Arab, Muslim friends, that they are being singled out, and some of them with great embarrassment, men and women, are being stopped not for a strip search but for lengthy interrogation and for searching of their belongings. Many of them are reputable business people who have been established in the Chicago community for 10, 20 years, who have businesses with many employees. And travel has become an opportunity for harassment. And I understand the line of this questioning when it relates to laptops, but I also want to go to the larger issue of profiling and elicit some comments from you relative to that.

Ms. Khera, does the DHS policy allow for Arab and Muslim Americans to be singled out for scrutiny on the basis of their national origin or religion?

Ms. KHERA. Senator Durbin, you raise an excellent question and let me also first say—just thank you for your leadership on this issue. I know back 10 years ago when these issues arose involving the U.S. Customs Service, you led the fight here in Congress in trying to hold the U.S. Customs Service, the predecessor to the CBP, accountable at that time. So thank you for your continued interest in these issues.

We believe that the current DHS guidance on this issue is not sufficient, that it does allow basically an escape hatch at the borders for DHS to use race, ethnicity. And what we heard this morning—in fact, I am very pleased to hear—is that there seems to be unanimity on this panel that singling Americans out based on their faith, ethnicity, is wrong and it is impermissible.

I think two things. One is I think it behooves Congress to make it clear that that is the case, because clearly lessons were not learned from the experience of 10 years ago, and I think we do need some very direct authority on this. And I know Senator Feingold has a bill on this issue, the End Racial Profiling Act. You have been also a strong supporter of that, and I think it behooves Congress to move on that legislation.

I think the second issue that this raises is even if in policy folks can agree that people should not be targeted, what is happening in practice, and are CBP agents receiving the kind of training they need and the proper guidance to ensure that they are not targeting people and not asking inappropriate questions.

And, finally, I would encourage Congress to conduct oversight, to be demanding of CBP the policy and guidance that is being given

VerDate Aug 31 2005 12:03 Nov 13, 2008 Jkt 045091 PO 00000 Frm 00030 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45091.TXT SJUD1 PsN: CMORC

to these agents, as well as having CBP provide Congress with information about the basis for why people are being subjected to secondary inspection, the kinds of questions that are being asked, and items that are seized, and if information is being seized, how it is being used, how is it being stored and shared.

Senator DURBIN. In this age of concern about security and terrorism, is it possible or even realistic to say that when it comes to these border situations, our Government cannot use race, religion, or ethnic background as the basis for searches or questioning?

Ms. KHERA. I think it is absolutely necessary for our Government to be clear that we are not targeting people based on those factors. I think those factors can be used in combination with other factors indicating some kind of criminal activity. So if there is, for example, a specific description of a suspect, a criminal suspect, or a specific terrorist who might be crossing the border, those factors can then be used. But as a general matter, it is not smart border policy. It is not fair as a matter of the Constitution, and it is not effective, because with the limited scarce resources, as even my colleague Mr. Carafano pointed out, CBP has scarce resources, and we need to be sure that CBP agents are using those scarce resources in an effective way and not targeting the family man who is returning home from a business trip to Japan with very invasive, intensive scrutiny. Because for every minute that is spent on targeting him, it is 1 minute less that CBP could be focusing on actual wrongdoers.

Senator DURBIN. Almost 4 years ago to the day, I asked then-DHS Secretary Tom Ridge in this Committee room about the special registration program, and he said at the time that he was going to modify or eliminate the program. Well, that has not happened in the 4 years since.

I would just ask this kind of general question to all the witnesses. Mr. Carafano, you testified that, "In order to be successful, CBP must avoid predictable patterns of behavior." This is the fundamental problem I see with profiling based on race, national origin, and religion. It is predictable, and terrorists and others seeking to do us harm can evade the profile once they learn about it.

So is there anyone here who disagrees with the premise that profiling on the basis of race, national origin, or religion may actually be counterproductive? Is there anyone who disagrees with that concept? Remarkable unanimity. I appreciate that very much.

Chairman FEINGOLD. Let the record reflect that no one disagreed.

Senator DURBIN. I would like to ask; is profiling worse at some airports in America than others? Testimony received today mentioned several instances in the San Francisco airport, and I wondered, obviously, if there had been any incidents at O'Hare or other airports.

Ms. KHERA. Senator, the complaints that we have received and other civil rights organizations have received have come from a number of different airports and land crossings. That includes San Francisco, Seattle, Newark, Houston, Boston, as well as land crossing in Detroit and the Washington State-Canadian border. So it has been a variety of different locations.

Senator DURBIN. So it is not one particular airport. It is many.

Ms. KHERA. Yes.

Senator DURBIN. Thank you very much, Mr. Chairman. I appreciate it.

Chairman FEINGOLD. Thank you, Senator Durbin. I will begin another round.

Professor Swire, DHS's written testimony asserts that CBP border searches have helped to identify terrorists attempting to enter the United States. The testimony does not mention whether or not these laptop searches could have proceeded even if a reasonable suspicion standard were in place. In the few specific examples that are mentioned, it seems abundantly clear that reasonable suspicion was present, and so a reasonable suspicion requirement would have not interfered with apprehending these individuals.

The same is true of Zacarias Moussaoui, whom Professor Sales mentioned in his testimony. In Moussaoui's case, an FBI agent determined that there was a 50-percent probability his computer contained evidence of criminal activity. Although this was considered insufficient for probable cause, it surely was enough for reasonable suspicion.

Do you think requiring a reasonable suspicion threshold for electronic searches will result in terrorists slipping through our fingers?

Mr. SWIRE. Mr. Chairman, I think the reasonable suspicion threshold is a sensible and traditional legal way to go here. Maybe I can just briefly make a response to Senator Brownback, who asked earlier whether there is any distinction we can make between digital cameras and digital laptops and the rest.

I think there is an important distinction that was not highlighted yet, which is that with digital things you do not just get a border search; you get a permanent search, that there is a record kept and a searchable data base created. And that does not happen with a suitcase, but it happens with these digital things. So the permanent search and the ability then to move it around the information—sharing environment makes all of these searches very different from traditional other searches. It is an additional clear legal reason to have a suspicion before these searches happen.

Chairman FEINGOLD. Did you want to respond to the part of my question about reasonable suspicion?

Mr. SWIRE. Reasonable suspicion. So I think in answer to your question, my reading of the cases is that the examples pulled out about terrorism involve reasonable suspicion. And I have not quibbled with and I believe in your opening statement you made mention that reasonable suspicion is an acceptable basis for searches at the border. It is random or suspicionless searches that the business travelers and the rest of us have very severe concerns about, and it is the one—suspicionless searches are the ones that pose the biggest computer security and general infrastructure risks.

Chairman FEINGOLD. On that point, Ms. Khera, we have heard testimony from Ms. Gurley about the practical harms of subjecting business travelers to laptop searches, including the increased cost to companies and loss of competitive edge for our country. What is the harm that we suffer as a nation when Americans are singled out for intrusive searches and questioning because they are Muslim or because they are of Arab or South Asian descent?

Ms. KHERA. Mr. Chairman, first let me make it clear that I think all Americans, including Muslim-Americans, certainly are willing to put up with some inconvenience to ensure that our country is safe and secure. And I think what we are talking about is not just mere interference but some activities questioning searches that actually go beyond and really in some cases result in hours of being detained and being interrogated, and we have at least one case where the actual property, the cell phone was actually returned in a damaged and inoperable condition. So there is some very specific harm to individuals. And I would say in terms of more broadly speaking, in terms of your question about the harm to our country, I think fundamentally this is an issue of is this an effective—are these effective tactics? And is the broad power of the CBP being used to actually focus on the bad guys? Or are they really, you know, following the leads, following the actual evidence, facts indicating criminal activity? Because, again, we have scarce resources, and in order to be safe and secure, we need our resources being used in a targeted way going after the bad guys.

Chairman FEINGOLD. Thank you.

Professor Swire, if we assume, just for the sake of argument, that the Government has always had the right to read any document that citizens carry with them across the border, travelers in the past could avoid that situation by choosing not to take sensitive documents with them on their travels. Now, is that a practical option for most traveling Americans—to just leave their laptops at home or delete any private information before traveling?

Mr. SWIRE. It does not seem a very good option, and they impose costs on travelers if they have to get a second laptop or get a second BlackBerry or whatever.

Something that Dr. Carafano said earlier is that the border people will be limited by resources so they will not copy very much, they will not do this very much. But the cost to copying and storing data is going down to close to zero. We have technology to just make it a routine thing to copy at the border, and part of the reason to have this hearing now is before we get to that point, we should have procedures in place.

Chairman FEINGOLD. Ms. Gurley, Mr. Cunningham testified that American citizens have no reasonable expectation of privacy in the contents of their laptops at the border because the country from which they have traveled may have searched the laptops as well. He states, "I submit that many countries conduct much more aggressive searches than the United States."

Is that consistent with what the members of your organization have experienced in their business travel? Do other countries examine the contents of laptops without individualized suspicion?

Ms. GURLEY. I believe that Canada has similar regulations to us, but I assume that countries like Uzbekistan, North Korea, and other countries search your laptops, but I do not think that should be our benchmark.

Chairman FEINGOLD. Thank you.

Senator Brownback?

Senator BROWNBACK. Thank you, Mr. Chairman.

Dr. Carafano, you said in your written testimony that there are numerous instances where we have gathered crucial information

from terrorists' laptops. Could you give us a couple of examples of where that has happened?

Mr. CARAFANO. Absolutely, Senator. I would just like, if I may for the record, Professor Swire said that I was talking about costs on the border. I was primarily referring to costs of individuals and the time of the individual agents at the border. I was not talking about the cost of, you know, taking and storing data.

Senator BROWNBACK. With costs at the border for as far as that there is the time of inspection of the people?

Mr. CARAFANO. That is absolutely the most critical element because there are two costs there. There is, one, the cost of the agent. You are taking—you are occupying the time of that agent and secondary inspection, focusing him on an individual. So that is the most—that agent is the most important in the line of defense at the border of making the determination of whether this person is a high-risk traveler, how much time should be spent with them, you know, how much of a risk do they actually—how much questions you need to ask, how much do you need to determine probable cause, because maybe you need to make a more intrusive inspection. So that is an incredibly valuable asset, and that is the real time we are concerned about.

And the second—

Senator BROWNBACK. Just on that, how many border crossings a year happen into the United States by U.S. citizens?

Mr. CARAFANO. Millions.

Senator BROWNBACK. Does anybody know the actual number?

Mr. CARAFANO. Tens of millions.

Senator BROWNBACK. I thought I had seen at one point in time that we had legal crossings a year into this country of over 200 million. Legal crossing into the country per year.

Mr. CARAFANO. That may be if you want to count citizens or the number of times they actually cross the border. Some people in San Diego, for example, cross the border several times a day, and every one of those counts as a crossing.

Senator BROWNBACK. I guess my point of that—and I do not know how many border agents we have that do that actual inspection. Does anybody know that actual number?

Mr. CARAFANO. Well, it depends. For example, at L.A. Long Beach, there are about 1,500 CBP agents at the port of L.A. Long Beach, give or take, doing not just border inspections, not just inspecting people, but cargo and everything else.

Senator BROWNBACK. It has been my experience that a lot of people cross these borders every day, and so what you are talking about is just a practical effect of agents looking, and that is your primary line of defense right there, is pretty limited about the amount of time that they have per person and decisionmaking that they have.

Mr. CARAFANO. That is correct, Senator. And the other great concern we have is the travelers themselves. The more time they spend at the border, the higher the transaction costs of crossing that border for them and their company and the people that they serve. So you want to reduce those down to the minimum you possibly can, but you want to make sure that your security concerns are absolutely looked after. And so that is why you want to focus

those assets on the high-risk travelers. And you are going to use a range of resources to do that from intelligence gathering to sharing of information. And that is why these initial searches are an important part of that whole thing.

I do think it is important that we make a distinction between an intrusive search, which does require probable cause, and what you would call a suspicionless search or inspection. You know, generally, even suspicionless searches and inspections are bad because they increase transaction costs. But that is not always the case. There is one category of suspicionless search or inspection that makes perfect sense, and that is a random inspection because, remember, what you are trying to do is just not speed travelers through, you are trying to identify bad guys. And part of catching the bad guy is making sure that they cannot identify the patterns of inspection that you are using. So randomness is an important component of that.

For example, we have a Container Security Initiative. We inspect a percentage of high-risk cargo coming into the United States. But occasionally we will just pull off a container and just x-ray it for no other reason, just to try to make it more difficult for people to identify the pattern of characteristics that we are looking for to identify high-risk behaviors.

So, again, to make that inspector at the border the most efficient and effective possible, we do have to be concerned about two things. One is we cannot make his trade craft so transparent that the terrorist or criminal can say, Oh, I will just do this and I will walk through. And the other thing is we have to give him the discretionary authority that he needs so he can focus his resources on the high-risk travelers. Again, the way we do that is to maximize the human capital investment we make in them so they are not doing racial profiling, maximize the technology they have available so they can get the information they need to identify high-risk travelers. But equally important is to provide them the flexibility they need in doing searches that are not intrusive, to be able to identify who are the people they should focus on.

Senator BROWNBACK. Give me a couple of examples of what we have caught on terrorists' laptops.

Mr. CARAFANO. I think that is a great question because I think it is unquestionable that technology can be a formidable weapon. I mean, the most startling examples, of course, are not actually border-crossing incidents, but, for example, when we went into Pakistan and uncovered computers which had enormous data on al Qaeda operations. The computers and records that have been looked at, for example, in regards to A.Q. Khan and forensically what we have been able to determine about the terrorist network that they use for the movement of people and material is huge. So the fact that a technology like a computer can be a weapon and can contain an enormous amount of material that indicates malicious and criminal activity, I do not think that is disputable.

Senator BROWNBACK. Thank you, Mr. Chairman.

Chairman FEINGOLD. Just a couple more questions from me.

Mr. Tien, as you know, the Constitution prohibits searching an American citizen's laptop within the borders of this country without probable cause and a warrant. If no limits are placed on cus-

toms officials' ability to search laptops at the border, what is to stop law enforcement agencies from staging an end run around the constitutional requirement of a warrant by requesting that customs officials perform the search the next time that individual attempts to travel overseas?

Mr. TIEN. I am afraid that there is not any current limit on that, and we have actually seen cases in which it appears that individuals are searched when they come back from international travel because there is some sort of vague red flag alert in the data base that says "put this person into secondary screening and then search." The cases are not always clear on the actual reason why that flag was in there. It is just, "pull this guy over."

So we are very concerned that this problem of suspicionless searches does not require that everyone be searched. It can simply be that the Government is abusing its authority to pick out people based on factors that would not support probable cause in the United States.

Chairman FEINGOLD. Thank you.

Professor Swire, I was struck by your comparison to the encryption wars of the 1990s, which I found quite apt. One particularly compelling point you made was the ultimate futility of anti-encryption rules in achieving the intended goal of preventing the use of strong encryption. You drew a comparison to laptop searches, stating that "moderately smart criminals and terrorists" would be able to avoid having electronic information captured through border searches.

Can you elaborate on why you do not think laptop searches will be particularly helpful in apprehending competent criminals and terrorists?

Mr. SWIRE. Thank you, Mr. Chairman. If we assume moderate intelligence and the ability to do searches on the Internet for today's hearing transcript, the first thing that you do if you are trying to avoid the border is you do not carry things in your laptop. You can load your files in heavily encrypted form up to a server, and then when you get to the far side, you download it from the server, and there is never anything in your laptop when you cross the border.

The second trick is using TrueCrypt or other software that is easily available today in the public market, widely used. And what you do then is you take your laptop, and when the agent says, "Open it up and give us your password," you open it up, but there is a second layer of encryption so the directory does not show the hidden part of your hard drive that has the other things hidden in there.

That does require you to lie to the Border Patrol officer, so the Border Patrol officer says, "You can see everything here?" And you say, "Oh, yes, sir, it does." But at a technological level, the Border Patrol agent has gotten in partway to your computer but cannot get the rest of the way in. So that is two ways through that are widely known today.

Chairman FEINGOLD. Senator Brownback, did you want to followup?

[No response.]

Chairman FEINGOLD. First let me thank Senator Brownback for his very—

Ms. KHERA. Mr. Chairman, do you mind if I—

Chairman FEINGOLD. Very briefly, please.

Ms. KHERA. Just a brief comment, because in Dr. Carafano's last statement, he was mentioned Pakistan and laptops that have been found in possession of al Qaeda with various material. And I think it is just worth clarifying that the community has been concerned that the DHS is using the factor of which country people have traveled to as a potential basis for singling out people, and I just wanted to clarify that the kinds of stories we hear around the Muslim community do not seem tailored to the issue of trying to determine whether there is somebody who has been mingling with al Qaeda in Pakistan and potentially carrying laptops. You hear questions about the political views, Presidential candidates, how often they pray, their associations with people in the United States, and it seems to be tied not to criminal activity but instead some part of some broader intelligence-gathering exercise. So I just wanted to clarify.

Chairman FEINGOLD. Fair enough, and as luck would have it, or I guess the world we live in, I am trying to get to a Foreign Relations hearing on Pakistan right now. So I want to thank all the witnesses for their testimony. I think it is extremely important to start giving close examination to this issue because we are to some degree in uncharted legal territory. I appreciate Senator Brownback's active and valuable participation in the hearing.

As I mentioned at the beginning of the hearing, neither the Framers of the Fourth Amendment nor the Supreme Court when it crafted a broad border search exception could have conceived of a world in which Americans crossed over the border dozens of times each year, carrying with them virtually all of their personal information. It is time for the law to catch up with reality. This hearing has shed some light on what that reality is and how ordinary law-abiding Americans are affected when the Government claims an unlimited right to search their laptops.

There is room for common sense here. I suspect everyone in this room who is learning about these searches for the first time had a visceral reaction to the idea of the Government reading through the contents of their laptops, browsing their e-mails, and looking to see what websites they have visited. That reaction, I am guessing, was very different from the reaction they would have if asked to open their suitcase. In my opinion, these different reactions demonstrate the need for different policies.

I also think this issue has to be placed in the larger context of this administration's ongoing assault on Americans' privacy. There was a statement in Mr. Cunningham's written testimony that I found breathtaking. He said, "Given the possibility of surveillance of phones and the Internet, 'old-fashioned' smuggling across the border, by storing files on a laptop, might prove a safer and more attractive alternative for [terrorist] communication provided the persons doing so could be assured that the computer would not be subject to the possibility of random and suspicionless search." The implication is that the way to stop terrorists is to ensure total Gov-

ernment surveillance authority over every person at every point, both inside our borders and out.

That is certainly one way we can respond to the threat we face from terrorism. We can become a surveillance state. But I remain convinced that a better approach is to remain true to our core values as a Nation. I do not think that suspicionless searches of Americans' laptops at the border or anywhere else are consistent with those values, nor do I think they are an effective means of fighting terrorism.

Many of the witnesses today had ideas for solutions that would bring border searches back in line with our values and our constitutional principles. I will be taking a close look at these ideas in the weeks ahead. Because of the upcoming holiday recess, the hearing record will remain open for 2 weeks for additional materials and written questions for the witnesses to be submitted.

As usual—

Senator BROWNBACK. Mr. Chairman, I want to make a closing comment.

Chairman FEINGOLD. OK. Why don't you go ahead and then I will finish.

Senator BROWNBACK. Mr. Chairman, I was not going to make a closing comment, but with yours, I think it is appropriate as well to also draw some balance on this. I think this is a good topic for us to discuss. It is an important one. I think you also get a little stretching on the administration's—they are just trying to search everybody. I think you have got a very practical concern here that we are trying to protect, the people are trying to protect the country, and that you have got hundreds of millions of crossings a year. You have people attempting to come into the country or from the country to do us harm, and you have got a real security need that is here. I think you have a court that has responded to this, that it has addressed some of the issues right at the border and your standards of review that exist at that border.

I would hope people would look at that in a balanced sense and would say, OK, we do have legitimate—there are legitimate security needs, standards at the border have been established by the courts, and we need to see some practical implementation of that where you have hundreds of millions of people crossing the border. I cross the border on not an infrequent—a couple of times a year, and I think we can be sensible about that without just the hyperbole of blaming an administration that wants to have a surveillance state. They do not want to have a surveillance state. Nobody wants to have that. Nobody wants to stand for that. But we do want to try to keep the American people safe. And it is just a very practical thing that I hope we could work on a practical basis, protecting those constitutional rights, recognizing the difference that the Court has articulated at the border, and try to work that on forward.

Thank you, Mr. Chairman.

Chairman FEINGOLD. Let me simply conclude by saying I wish that what I said about the administration was extreme. But it is not. This administration for years has created an environment, whether it be the Inspector General's reports about the detentions of Muslim-Americans and others right after 9/11 or any number of

other practices—you name it. They have created this environment where, frankly, people might believe a level of surveillance and activity that is even beyond reality. We are going to have a new administration, whether it is Republican or Democrat, but the historical record is clear that this administration has been reckless with regard to the privacy of the American people. And I realize we disagree on that, and this was not the focus of the hearing, but I believe that if we are going to fix all this, we need to have a different environment with regard to the next administration. I am hoping we get that.

As usual, we will ask the witnesses to respond promptly to any written questions so that the record of the hearing can be completed. Thank you.

This hearing is adjourned.

[Whereupon, at 10:49 a.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

st. john's UNIVERSITY

Larry Cunningham
Assistant Professor of Legal Writing

Direct (718) 990-7616
E-mail CUNNINL1@stjohns.edu

School of Law

Tel (718) 990-6600
Fax (718) 591-1855
8000 Utopia Parkway
Queens, NY 11439
www.law.stjohns.edu

July 29, 2008

Via e-mail to margaret_whiting@judiciary-sem.senate.gov
Margaret Whiting
United States Senate
Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C. 20510-6275

Dear Ms. Whiting:

I am writing in response to two written questions from Senator Brownback with regards to my testimony before the Subcommittee on June 25, 2008, on the subject of border searches.

1. "In his closing statement, Chairman Feingold indicated that your testimony contemplated a surveillance state, based on your statement that, '[g]iven the possibility of surveillance of phones and the Internet, "old fashioned" smuggling across the border, by storing files on a laptop, might prove a safer and more attractive alternative for such communication provided the persons doing so could be assured that the computer would not be subject to the possibility of random and suspicionless search.' I'd like to give you the opportunity to respond to this characterization of your testimony."

I was surprised by this statement from Chairman Feingold and his insinuation that I approved of all of the Bush Administration's tactics in the War on Terror ("I also think this issue has to be placed in the larger context of this administration's ongoing assault on Americans' privacy. There was a statement in Mr. Cunningham's written testimony ..."). In fact, my written testimony indicates the need for restraint and balance in this area. I specifically distinguished searches of laptops from their seizure:

> Seizures of such devices are another matter altogether. The border exception justifies the search, not the seizure, of items that cross the border. In order to seize an item, the government must have probable cause that the item is, or contains, contraband. If a Customs officer finds child pornography on a laptop, for example, he or she would be justified

> in seizing the computer since it contains contraband and persons do not have a right to retain contraband. I am aware of no authority that would permit the government, without probable cause to believe it contains contraband, to keep a person's laptop or to copy the contents of its files.

Moreover, because of the privacy concerns at issue with laptop searches, I suggested the need for oversight, established procedures, training, and supervision:

> During oral argument in *Flores-Montano*, it came to light that Customs keeps a record of all border searches that its agents conduct and the reasons, if any, for each particular search. If this is the still the case, the records should provide Congress with enough information to determine whether laptop searches are being conducted in a abusive or racially discriminatory manner. . . . If such records are no longer being kept, it might be advisable for the practice to be restarted.
>
> The Executive Branch can take administrative and rule-making steps, in addition to record-keeping, to ensure that privacy intrusions are kept to a minimum. For example, at the traveler's request, an examination of a computer should occur away from public view. Only officers who have received appropriate training should be allowed to conduct searches, in order to minimize the possibility of irreparable damage to, or erasure of, files and the hardware itself. A rule requiring searches to be conducted in the presence of a supervisor would also be prudent.

My testimony, therefore, was a far cry from calling for a "surveillance state."

Regarding the specific portion of my written testimony that Chairman Feingold quoted, my statement was not intended to argue for the creation of a "surveillance state." Rather, my point was that terrorists might use laptops and other electronic storage devices to bring messages or plans into the country if they knew that there would be a lower risk of detection than through, for example, phone calls, e-mails, or instant messages. The fact is that surveillance of Internet traffic and telephone communications can legally occur through wiretaps and other electronic intercepts. I expressed no opinion in my written testimony about the legality or desirability of specific forms of surveillance or whether the Executive Branch may employ such methods without judicial review. (In fact, my personal view is that, in the absence of severely exigent circumstances, any surveillance of telephone conversations or Internet traffic should first be preceded by a warrant, obtained from either a judge of the Foreign Intelligence Surveillance Court or any another Article III judge. I was troubled when the *New York Times* reported, in late 2005, of an Executive Order authorizing National Security Agency wiretaps without FISC approval. In my view, the FISA process works well and provides a necessary check against overzealous government conduct.)

2. "In your written testimony, you indicate that travelers entering the United States have a lowered expectation of privacy in the objects and papers they bring with them, in some part because those objects and papers may have been subjected to search—and even extensive search—by the country they are leaving. In response to questioning from Chairman Feingold, Ms. Gurley testified that the United States should not base its border search policies on the examples of countries like North Korea and Uzbekistan. Is it your understanding that only totalitarian nationals like these conduct proactive border searches?"

No. In fact, before mentioning North Korea and Uzbekistan, Ms. Gurley testified that Canada, like the United States, has a practice of searching laptop computers at the border. Indeed, in *United States v. Romm*,[1] the defendant's child pornography was initially found during an entrance search by Canadian officials. A brief examination of the laptop indicated that its Internet browser's "history" folder contained the images in question. After Canada refused the defendant entry, he was returned to the United States where our customs officials searched his laptop, found ten images of child pornography, and made a formal arrest. Without the proactive work of Canadian law enforcement, the defendant—who had a criminal history of sex offense convictions—may never have been caught. This example demonstrates that the United States is not alone in this area and that even respected democracies, like Canada, take steps to protect their borders.

There is a broader point here, however. A basic question in this area is: how much of a reasonable expectation of privacy does a person have while traveling internationally? An international journey will, by definition, require contact between the traveler and at least two countries, the origin nation and the destination nation, each of which has a right to conduct its own entrance and exit search. An American traveler should therefore recognize that even if the United States adopted a relaxed border search policy, he and his possessions would still be subject to search by the other countries with which he had contact. A prudent traveler, concerned for the privacy of his person and belongings, would limit the sensitive information he carries while traveling abroad. Indeed, the U.S. Department of State, on its website,[2] cautions travelers against bringing unnecessary papers or objects on international trips. It also advises travelers to check with the foreign country's embassy to determine which items are prohibited by local law.

My point is *not* that we should mirror the policies and practices of totalitarian nations. Rather, all countries conduct both entrance and exit searches as a matter of course. Therefore, a change in U.S. border search policy would not, by itself, diminish the privacy intrusions that travelers would face.

* * *

[1] 455 F.3d 990 (9th Cir. 2006).

[2] http://travel.state.gov/travel/tips/tips_1232.html

Thank you for the opportunity to submit these written answers into the record. Please advise me if you require anything additional.

Sincerely,

Larry Cunningham
Assistant Professor of Legal Writing

MUSLIM ADVOCATES
PROMOTING FREEDOM & JUSTICE FOR ALL

July 30, 2008

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

Senator Feingold:

Please find attached responses to each of the questions submitted by your office on July 15, 2008, following the June 26, 2008 hearing in the U.S. Senate Judiciary Committee Subcommittee on the Constitution regarding "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel."

Respectfully submitted,

Farhana Khera
President & Executive Director
Muslim Advocates

U.S. 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

Responses by Farhana Khera, President & Executive Director, Muslim Advocates To Written Questions Submitted by Senator Feingold

1. **Some people might listen to your testimony and say, if a customs agent asked me intrusive questions about my religious and political beliefs, I would just refuse to answer, and then I would report the person who asked the question. Is it that simple? What sorts of real or perceived barriers exist for a Muslim American who wants to resist or protest this mistreatment?**

A number of real or perceived barriers exist for Muslim Americans who may want to resist or protest being asked about their religious or political beliefs by Customs and Border Patrol (CBP) agents. First, it does not appear optional that an American can refuse to answer questions about constitutionally protected beliefs and activities. All travelers need permission of the CBP agent in order to proceed beyond the screening area – and CBP agents frequently carry guns or other weapons that reinforce that message. In certain instances, CBP agents have actively intimidated travelers selected for scrutiny. (*See* Story #3, Written Testimony Submitted by Farhana Khera.) In addition, we are not aware of any guidance constraining a CBP agent from asking questions about religious or political beliefs or activities. Given the CBP's assertion of broad authority, we are concerned that refusing to answer questions can result in further delay for the traveler and/or more extensive searches, as well as being entered into a CBP database and flagged for intensive scrutiny the next time he or she re-enters the U.S.

Second, many Americans are not aware of their rights and the scope of permissible questioning. In response, Muslim Advocates has conducted "know your rights" sessions in the Muslim American community and recently produced an educational video for community members to inform them about their rights at the border and the scope of permissible questioning. (This video is available on our website and in DVD.) The video specifically addresses the issue of impermissible questioning about religious or political beliefs and lawful associations.

Third, Muslim Advocates encourages travelers to record the name and badge number of CBP agents and supervisors and to file complaints if they have not been treated fairly. But Muslim Advocates has found that many Muslim Americans are reluctant to file complaints because they fear retaliation and even greater scrutiny by law enforcement.

Finally, even if travelers file complaints, Muslim Advocates is concerned about the failure to have these complaints meaningfully resolved. Nearly every traveler

summarized in the written testimony submitted by Muslim Advocates for the record of the hearing had filed a complaint with the U.S. Department of Homeland Security (DHS), but not a single one of these complaints has led to a resolution and improvement in the traveler's experience.

2. The written statement that DHS provided the night before the hearing states as follows: "[A]n individual's frequent travel to countries associated with significant terrorist activity, narcotics smuggling, or sexual exploitation of minors, may give our officers reason to question that person's reasons for travel. When officers are satisfied that the person has valid reasons for the frequent travel, and there are no other areas of concern or potential violations, the person may be cleared to enter the United States." Does this address your concerns as to whether customs agents are targeting travelers based on their race, ethnicity, religion, or national origin?

No. The Department's statement does not address our concerns and is insufficient to allow Congress and the public to fully assess how travel patterns are being used in selecting individuals to subject to more intensive questioning or searches. Based on what we do know, information about a traveler's travel patterns does not appear to be used fairly or effectively.

Specifically, the Department states that when "there are no other areas of concern or potential violations," the traveler may be cleared to enter the U.S. What are these "other areas of concern"? What are the "potential violations"? What guidance does DHS and CBP provide line agents in determining "other areas of concern"? Based on the Department's statement, there appears to be enormous discretion and subjectivity by CBP in selecting whom to screen more closely. We therefore urge Congress to request information from DHS and CBP about how information regarding travel patterns is being used.

In addition, Congress should inquire about the guidance and training CBP has given its agents, including the levels of guidance and training provided to agents when intelligence directives have been issued by DHS or senior CBP officials. Adequate training curricula and materials are necessary to ensure that CBP agents understand and implement policies and procedures correctly and fairly.

Furthermore, based on the complaints received by Muslim Advocates, the government appears to have a very broad definition of "countries associated with significant terrorist activity, narcotics smuggling, or sexual exploitation of minors." Witnesses have reported encountering scrutiny when traveling from places as diverse as Japan (story #1), Canada (stories #1, #3, #8); Turkey (story #1); and even a trip to Jordan sponsored by the U.S. Department of State (story # 9). DHS claims CBP applies a reasonable suspicion standard when evaluating potential threats, but such assurances do not answer why a law-

abiding corporate lawyer with a Georgetown law degree was singled out and interrogated about subjects including her views of presidential candidates (story # 2).

Based on complaints received, Muslim Advocates is concerned that travel patterns could be a proxy for religion or ethnicity in selecting travelers to subject to additional scrutiny. This would be wrong and improper, although not necessarily a violation of DHS guidelines implementing the U.S. Department of Justice (DOJ) Guidance banning racial profiling since the DOJ Guidance and DHS guidelines created an exception for compelling governmental interests (e.g., national security) that swallows the rule banning profiling. That is why federal legislation clearly banning racial, ethnic and religious profiling is needed.

Finally, Muslim Advocates also urges Congress to require CBP to collect data about individuals who are selected for more extensive questioning and searches and the basis for doing so. Rigorous data collection and reporting will help both the agency and Congress monitor the activities of CBP at the border and ensure that discriminatory targeting of travelers based on their faith, ethnic or racial background is not taking place.

3. As you noted in your testimony, DHS policy is to "prohibit the consideration of race or ethnicity in our daily law enforcement activities in all but the most exceptional instances, as defined in the DOJ Guidance. DHS personnel may use race or ethnicity only when a compelling governmental interest is present."

a. In your view, what "compelling governmental interest" would justify DHS personnel relying on race or ethnicity in deciding whom to subject to intrusive border searches?

CBP agents have an important responsibility to protect our borders but they also have a responsibility to wield that power fairly and effectively. Absent a suspect-specific description, reliance on race or ethnicity should not be permissible in deciding whom to subject to intrusive border searches. Americans are guaranteed equal treatment and equal protection under the laws by the federal government – that includes federal officials at the border. Congress should enact legislation requiring CBP to focus on real threats and ensuring reporting and accountability to Congress.

b. Do you believe that DHS's laptop search policy is consistent with the DOJ Guidance?

Based on what DHS has publicly disclosed about its laptop search policy, it does not satisfy concerns about whether CBP may be engaging in inappropriate targeting of travelers based on race, ethnicity or religion. First, the DOJ Guidance is inadequate because it explicitly exempts any investigations predicated on national security aims (including most border searches & interrogations). Moreover, the Guidance fails to address *religious* profiling, as distinct from racial and ethnic profiling. As discussed in the written testimony and in responses to questions 2 and 3.a. above, federal legislation banning racial, ethnic and religious profiling and requiring data collection and reporting by CBP is very much needed.

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 after 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 they shall have reason to suspect 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.

SUBMISSIONS FOR THE RECORD

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

Chairman Feingold, Ranking Member Brownback, distinguished Members of the Subcommittee, I am pleased to submit this testimony to you to discuss U.S. Customs and Border Protection (CBP) policies and practices with regard to searching the contents of laptops and other digital devices at our nation's ports of entry. My testimony today will provide you with specific information that the subcommittee has requested on how CBP inspects these items.

At the outset, I want to emphasize that CBP disagrees with the premise contained in this hearing's title: CBP's efforts do *not* infringe on Americans' privacy. It is important to keep in mind that CBP is responsible for enforcing over 600 laws at the border, including those that relate to narcotics, intellectual property, child pornography and other contraband, and terrorism. CBP's ability to examine what is coming into the country is crucial to its ability to enforce U.S. law and keep the country safe from terrorism. This notion is not novel. As the U.S. Supreme Court has stated, "since the

beginning of our Government," the Executive Branch has enjoyed "plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."

More recently, federal courts throughout the country have recognized that CBP's efforts at the border with respect to digital devices--like our efforts with respect to vehicles, suitcases, backpacks, containers of hard-copy documents, and other conveyances--are consistent with long-standing constitutional authority at the U.S. border and other laws.. This past April, in *United States v. Arnold*, the U.S. Court of Appeals for the Ninth Circuit upheld the suspicionless search of an international traveler's laptop computer that uncovered child pornography, stating that "[c]ourts have long held that searches of closed containers and their contents can be conducted at the border." Likewise, in 2006 a U.S. citizen was convicted following the discovery of child pornography on his laptop during a border search. The Ninth Circuit refused to vacate the conviction. And a similar conclusion was reached by the U.S. Court of Appeals for the Fourth Circuit in *United States v. Ickes*, which also involved a conviction for possession of child pornography.

In addition to several successes in arresting individuals possessing child pornography, CBP border searches also have been helpful in limiting the movement of terrorists, individuals who support their activities and threats to national security. During border searches of lap tops CBP officers have found violent jihadist material, information about cyanide and nuclear material, video clips of Improvised Explosive Devices (IEDs) being exploded, pictures of various high-level Al-Qaida officials and other material

associated with people seeking to do harm to U.S. and its citizens. These materials have led to the refusal admission and the removal of these dangerous people from the United States.

Another example of how a border search led to disruption of a national security threat is the case of Xuedong Sheldon MENG . In November 2004, ICE agents learned that MENG, a Canadian 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 are both controlled items for export under the AECA and the International Traffic in Arms Regulations (ITAR). On December 6, 2004, MENG traveled from China to Orlando, FL, to attend a defense conference. ICE agents coordinated with CBP to conduct a border search of MENG and his belongings when he entered the United States at Minneapolis, MN. During the search, CBP officers identified a laptop computer and portable hard drive belonging to MENG. A preliminary search of the laptop revealed that it contained software belonging to the American company which is a controlled item for export under ITAR.

On June 18, 2008, MENG, was sentenced in the Northern District of California to two years incarceration for violations of 18 USC 1831, the Economic Espionage Act; and 22 USC 2778, the Arms Export Control Act. MENG also received a $10,000 fine and 3 years probation. Additionally, this is the first ICE case involving a conviction under 18 USC 1831. This is also the first conviction and sentencing for violations of 22 USC 2778 involving computer software. This joint ICE and FBI investigation was made possible by information gained by the initial CBP border search of his lap top and portable hard drive.

CBP and Immigration and Customs Enforcement (ICE) continue to carry out border searches within their legal authorities and have been able to arrest criminals and limit the entrance of dangerous people to the U.S. as a result. To treat digital media at the international border differently than CBP has treated documents and other conveyances historically would provide a great advantage to terrorists and others who seek to do us harm. As the U.S. Court of Appeals for the Second Circuit stated in the case *United States v. Irving*, which upheld the border search of luggage and a subsequent search of a camera and computer diskettes, treating the computer diskettes differently than other closed containers "would allow individuals to render graphic contraband, such as child pornography, largely immune to border search simply by scanning images onto a computer disk before arriving at the border." The same could be said for terrorist communications. Indeed, the Fourth Circuit in *United States v. Ickes* rejected an argument that additional protections should apply to certain material contained on computers, stating that this logic "would create a sanctuary at the border" for all such material, "even for terrorist plans."

As America's frontline border agency, CBP employs highly trained and professional personnel, resources, expertise, and law enforcement authorities to meet our twin goals of improving security and facilitating the flow of legitimate trade and travel. CBP is responsible for preventing terrorists and terrorist weapons from entering the United States, for apprehending individuals attempting to enter the United States illegally, and stemming the flow of illegal drugs and other contraband. We also are protecting our agricultural and economic interests from harmful pests and diseases and safeguarding American businesses from theft of their intellectual property. Finally, we

are regulating and facilitating international trade, collecting import duties, and enforcing United States trade laws.

One goal of the CBP inspection process is to establish that a person attempting to enter the United States does not pose a threat to the safety and welfare of our nation. Our ability to search information contained in documents and electronic devices, including laptops, is just one enforcement tool aimed at defending against these threats. As you know, all persons, baggage, and other merchandise arriving in or departing from the United States are subject to inspection and search by CBP officers. As part of the inspection process, officers verify the identity of persons, determine the admissibility of aliens, and look for possible terrorists, terrorist weapons, controlled substances, and a wide variety of other prohibited and restricted items. Every person seeking to enter the United States must be examined by a CBP officer at a designated port of entry. This may include checking names and conveyances in law enforcement databases; examining entry and identity documents; examining belongings and conveyances; collecting biometric information where applicable; and questioning the traveler.

Aliens have the burden of establishing that they are admissible to the U.S., or are entitled to the immigration status they seek. U.S. citizens also have to establish their citizenship to the satisfaction of the officer and may be subject to further inspection if they are the subject of a lookout record, if there are indicators of possible violations (such as the possible possession of prohibited items, narcotics, or other contraband), or if they have been selected for random compliance examination.

At the Senate Judiciary Committee's hearing on the oversight of the Department of Homeland Security (DHS), held on April 2, 2008, a question was asked about the

inspection of individuals with connections to countries associated with significant terrorist activity. At that hearing, Secretary Chertoff stated that, "U.S. citizens are not treated differently based upon their ethnic background, but their individualized behavior could be a basis for singling them out, or if they matched a physical description it could be a basis for singling them out." One of the primary objectives of the CBP inspection process is to establish that a person is lawfully entering the United States, and does not pose a threat to the safety and welfare of our nation. Thus, an individual's frequent travel to countries associated with significant terrorist activity, narcotics smuggling, or sexual exploitation of minors, may give our officers reason to question that person's reasons for travel. When officers are satisfied that the person has valid reasons for the frequent travel, and there are no other areas of concern or potential violations, the person may be cleared to enter the United States. There are no special rules for personal belongings or documents. However, CBP does enforce numerous laws concerning material in paper or electronic form, both of which are treated the same conceptually and constitutionally. For example, U.S. laws prohibit the importation of child pornography, that constitutes pirated intellectual property, or that contains any threat to take the life of or inflict bodily harm upon any person.

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.

One example of an instance where CBP determined it necessary to conduct a search of a laptop computer and other electronic equipment occurred on July 17, 2005, when a Michael Arnold arrived at Los Angeles International Airport on a flight from Manila, Philippines. Mr. Arnold was selected for a secondary examination, and exhibited nervous behavior when questioned about the purpose of travel to Manila. After failing to provide consistent answers about the individual's occupation and purpose of travel, a declaration was obtained and the individual's luggage was inspected. Upon the inspection of the laptop and CDs found in the individual's luggage, officers found images of adults molesting children. U.S. Immigration and Customs Enforcement (ICE) then conducted an interview of the individual and searched the contents of the individual's laptop, CDs, and memory stick. These items were detained, and turned over to ICE for investigation. During his subsequent prosecution, the district court suppressed the evidence on the ground that the search violated the constitution. The government appealed, and the lower court's decision was overturned by the Ninth Circuit, which held that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." As the U.S. Supreme Court noted in the *Flores-Montano* decision in 2004, the Government's interest in preventing the entry of unwanted persons and effects – and the corresponding search authority of the sovereign – is at its zenith at the international border.

It is important to understand that CBP typically encounters well over a million travelers every day and is responsible for enforcing over 600 federal laws at the border. CBP does not have the resources to conduct searches on every laptop or cell phone that pass through our ports of entry, nor is there a need to do so. When we do conduct a search, it is often premised on facts, circumstances, and inferences which give rise to individualized suspicion, even though the courts have repeatedly confirmed that such individualized suspicion is not required under the law.

CBP's frontline officers and agents will continue to protect America from terrorist threats and accomplish our traditional enforcement missions in immigration, customs, and agriculture, while balancing the need to facilitate legitimate trade and travel. As I mentioned, the initiatives discussed today are only a portion of CBP's efforts to secure our homeland, and we will continue to provide our men and women on the frontlines with the necessary tools to help them gain effective control of our Nation's borders.

I would like to thank the Subcommittee, for the opportunity to present this testimony today, and for your continued support of DHS and CBP

Asian Law Caucus

Asian Law Caucus, Inc.
939 Market Street, Suite 201
San Francisco, CA 94103
Phone: (415) 896-1701
Fax: (415) 896-1702
www.asianlawcaucus.org

July 8, 2008

The Honorable Russell Feingold
Chairman
Senate Committee on the Judiciary
Subcommittee on the Constitution
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Sam Brownback
Ranking Member
Senate Committee on the Judiciary
Subcommittee on the Constitution
224 Dirksen Senate Office Building
Washington, DC 20510

Re: Subcommittee on the Constitution Hearing on "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel," June 25, 2008

Dear Senators Feingold and Brownback:

The Asian Law Caucus submits this statement in reference to the recent hearing on the invasions of privacy and infringements of civil liberties faced by Americans returning from overseas travel. We commend the Constitution Subcommittee for addressing this important issue, and we concur with the analysis and policy recommendations presented by the Electronic Frontier Foundation and Muslim Advocates to the subcommittee. We submit this comment in order to share additional stories of individuals affected by intrusive Customs and Border Protection practices and to expand on two issues: the First Amendment implications of Customs practices and the linkage between Customs practices and concerns over the terrorist watch list. We would appreciate if this statement could be made part of the record of the hearing.

I. Background on Asian Law Caucus

The Asian Law Caucus is a San Francisco-based nonpartisan, nonprofit organization that advocates for the legal and civil rights of Asian Americans and Pacific Islanders. The nation's first public interest legal organization serving the needs of the Asian American community, the Caucus has since 1972 championed the rights of individuals who have been denied civil liberties, victimized by hate crimes, or exploited by sweatshop employers. The Caucus has a long-standing commitment to national security policies that protect the equal rights and civil liberties of all American communities: the organization is perhaps best known for helping overturn the World War II-era conviction of Fred Korematsu for defying a federal order interning Japanese-Americans.

Since 2007, the Asian Law Caucus has received over two dozen complaints from U.S. citizens and residents who have faced lengthy detentions, invasive questioning about religious and political beliefs, or intrusive searches of laptop computers and other possessions by U.S. Customs and Border Protection. In response to the confusion and anxiety experienced in the South Asian, Middle Eastern, and Muslim American communities as a result of these practices, the Asian Law Caucus issued travel advisories to these communities in fall 2007 to educate individuals about their rights at land borders and airports.[1] In 2008, together with the Electronic Frontier Foundation, the Asian Law Caucus requested U.S. Customs and Border Protection to disclose its policies on border searches and questioning, and filed suit under the Freedom of Information Act when the agency failed to respond within statutory time limits.[2]

II. Incidents of Intrusive Searches and Questioning at U.S. Borders

The Asian Law Caucus continues to receive regular reports of travelers subject to intrusive searches of laptop computers, cell phones, digital cameras, and other electronic devices, as well as invasive questioning about religious practices, political views, and associations with friends and family. Community members who have called the Asian Law Caucus describe their experiences with Customs and Border Protection as intimidating and invasive, and they are shocked and disheartened to learn that the agency claims almost unfettered authority to conduct these practices.

These are some examples of individuals who have reported their experiences to the Asian Law Caucus:

- A U.S. citizen college professor in San Francisco who writes for national magazines was grilled about his travels to the Middle East and the notes he had taken while reporting on political events abroad. Agents removed his laptop computer to another room for 45 minutes and told him they were downloading all the files from his computer. When he protested his treatment, he was told, "This is the border, and you have no rights." His attempts under the Freedom of Information Act to find out what files Customs and Border Protection retained from his computer have so far been unsuccessful.

- A U.S. citizen in Sacramento, CA who works for a major high-tech company is repeatedly flagged for scrutiny at U.S. ports of entry, and told it is because he is "in the system." Customs agents have grilled him about his business travels, family members, and his views on current affairs in Syria and Israel. A Customs and Border Protection agent opened his corporate laptop computer and spent half an hour viewing websites he had visited, in addition to examining his cell phone directory, every item in his wallet, and other personal materials.

- A U.S. citizen IT consultant reported being questioned for almost 20 hours after five international trips, despite hearing an agent explain that he was not an actual match to a watch list. He was asked about his religion, whether he hated the U.S. government, whether he had visited mosques, and even told that he should "pray more." When he offered to give one agent his wife's phone number so the agent could verify his identity, he was asked,

[1] Copies of these advisories in English, Arabic, Urdu, Dari, and Hindi can be found at the Asian Law Caucus website at http://www.asianlawcaucus.org/site/alc_dev/section.php?id=99.
[2] Asian Law Caucus v. Dep't of Homeland Sec. (N.D. Cal., Feb. 7, 2008, No. 4:08-cv-00842-CW).

"Isn't it rude in Islamic culture to give a man a woman's phone number?" Customs agents inspected his company laptop computer, examined all the books in his luggage and recorded information on one book about the history of Islam, and prevented him from taking notes on the interview.

- The imam, or religious leader, of a Northern California mosque has been pulled aside ten times for questioning and extensive luggage searches when returning home to the United States. He is a U.S. citizen who participates actively in interfaith and civic work, including serving as a city human rights commissioner. On one occasion, when returning from a conference in Europe to which he had been invited by the U.S. government, agents examined a stack of business cards he had collected from other conference participants and took them to another room, leading him to suspect that the business cards may have been photocopied. As he wrote in a letter to federal officials, he teaches moderation, respect, and partnership with government agencies to his congregation, but his repeated experiences with Customs officials leads him to question why the government fails to accord him the same respect he urges community members to show law enforcement officials.

- A San Francisco mental health therapist who is a U.S. citizen was asked by Customs officials to name every person she had met and every place she had visited on a trip to the Middle East, including the names and addresses of all her family members abroad and the name, address, and occupation of her daughter in the United States. Her cell phone was removed from her possession, and she believes the record of her daughter's phone calls to her during that time was erased. She is an active member of her community: she co-founded an organization that promotes cultural harmony between Arab and American communities through education and the arts, and she established a racially diverse music ensemble to introduce Arab musical traditions to Americans. She reported feeling traumatized by her experience, worrying for days about the safety of family members and friends whose contact information she was compelled to provide Customs agents.

- A California businessman who is a U.S. citizen has been stopped, questioned, and searched numerous times upon his return to the United States. He has been asked what he thinks of Iran's president, whether he supports terrorism, whether he met any terrorists during the Hajj pilgrimage to Saudi Arabia, and what he thinks about Jews and the state of Israel. His laptop computer was removed from his presence for over two hours, and he was told that officers were examining all the files, including letters from his wife and children.

- A Silicon Valley marketing representative for a high-tech company has been stopped several times by Customs agents in the last two years. Agents questioned him about his volunteer activities at the mosque and searched his laptop computer on multiple trips, on one occasion asking him about websites he had visited. Because of prior searches, he now has stopped purchasing political books abroad for fear of being questioned about his reading habits; still, Customs agents recently questioned him on a book he carried on women's rights in Islam.

III. Chilling Effect on First Amendment Rights to Free Exercise of Religion, Free Speech, and Freedom of Association

Customs and Border Protection searches and questioning have a chilling effect on Americans' exercise of First Amendment rights to the free exercise of religion, freedom of speech, and freedom of association. As the examples above illustrate, numerous U.S. citizens and legal immigrants returning to the United States from overseas trips have faced questioning and searches that burden these First Amendment rights. Customs officials have grilled professors, filmmakers, business leaders, human rights activists, and software engineers alike on their political views, religious practices, and associations. According to travelers who have reported their experiences to the Asian Law Caucus, Customs agents have asked: What do you think of events in Syria and Israel? What's your opinion of Iran's president? Do you hate the U.S. government? Where do you worship? What kinds of political activism do you engage in? Do you volunteer at your mosque? What do you think about Jews and the state of Israel?

At the same time, Customs officials have forced returning travelers to hand over laptop computers, books, letters, digital cameras, confidential company documents, personal notebooks, cell phone SIM cards, and stacks of business cards collected from colleagues abroad. As they searched these materials, sometimes for hours, officers recorded the titles of books that travelers were reading, examined websites that travelers had viewed, downloaded files from laptop computers, questioned people about their personal contacts, and even read complaint letters that individuals had previously written to members of Congress.

Courts have long recognized that government practices short of prohibiting speech can substantially burden free speech and the exercise of other First Amendment rights. The chilling effect doctrine recognizes that "inhibition as well as prohibition against the exercise of precious First Amendment rights is a power denied to government."[3] But Customs searches and questioning have already deterred individuals from engaging in lawful expressive activities. For instance, as recounted above, one California high-tech worker who has been searched several times at San Francisco International Airport now refrains from bringing "political" books into the United States. Customs practices impinge on the "uninhibited, robust, and wide-open debate and discussion that are contemplated by the First Amendment."[4]

We are not aware of any Customs policies that constrain agents from questioning individuals on religious activities, political views, or other such topics. In January 2008, prior to filing its Freedom of Information Act lawsuit, the Asian Law Caucus convened a meeting with Customs officials in San Francisco in order to obtain information on whether such a policy existed. At that meeting, we were told that no black-and-white rules governed the questioning of individuals on political and religious subjects, but that a "fine line" separated appropriate and inappropriate questions. According to Richard Vigna, director of field operations for the Port of San Francisco, asking a U.S. citizen what mosque he or she attended was a "legitimate question." Leticia Romero, assistant director of field operations for border security, added that in contrast, the question, "How many times do you pray?" would probably not be appropriate.

---

[3] Lamont v. Postmaster General, 381 U.S. 301, 309 (1965) (Brennan, J., concurring).
[4] *See id.* at 307 (quoting New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)).

These answers demonstrate the need for a policy limiting Customs agents' inquiry into protected First Amendment activities. The examples given by Customs leadership in San Francisco suggest that the agency may be drawing a "fine line" in quite the wrong place: we believe that most Americans would be surprised to learn that Customs agents can question them about the place they choose to worship, without any indication of wrongdoing. Moreover, if top officials of the agency believe that it is legitimate to question Americans on their place of worship, it begs the question what individual Customs agents believe they are empowered to do.

Retention of records on Americans' First Amendment activities

Beyond the chilling effect created by border searches and questioning, the *retention* of information about Americans' religious and political activities in government databases would further burden First Amendment rights. In earlier eras in U.S. history, government agents assembled vast personal dossiers on the habits and beliefs of ordinary Americans in the name of national security. Reports from travelers and media investigations today raise similar concerns over the scope of today's Customs databases. A number of individuals reported to the Asian Law Caucus that they suspect, or were even told, that certain of their written materials or computer files were copied. In addition, the Washington Post reported last September that Customs has been collecting and monitoring detailed information about the travel habits of millions of Americans, including in some cases the books that individuals are reading, and storing this information for as long as 15 years.[5]

In *Heidy v. United States Customs Service*, a 1988 case involving Americans returning from Nicaragua, a federal district court found that Customs procedures for reading travelers' written materials and retaining information on them even after they were found not to violate U.S. law chilled travelers' right to free expression.[6] The court held that once Customs established that such detained materials were lawful, it must return all originals and destroy all copies, and could not provide other agencies with any copies unless the agency agreed to comply with this policy.[7] *Heidy* warned against "preserving a permanent record of persons who might be deemed to be 'subversive' or 'anti-administration'" premised exclusively upon the assumption that what one reads reflects what one thinks.[8]

Congress should ensure that the procedures for searching and questioning individuals, and creating records regarding these border inspections, do not chill travelers' rights to free speech, freedom of religion, and freedom of association.

IV. Impact of Mismanagement of Terrorist Watch List on Customs Searches and Questioning

The intersection of overbroad Customs and Border Protection practices with the mismanagement of the terrorist watch list exacerbates civil liberties threats to ordinary Americans. Not every individual subject to a laptop search or invasive questioning by Customs agents appears to have been flagged because of a watch list. Some travelers report a single incident of extensive search and questioning, suggesting that they may have been selected based on other factors or at the discretion of Customs agents. However, a number of individuals who have contacted the Asian

[5] Ellen Nakashima, *Collecting of Details on Travelers Documented*, WASH. POST, Sept. 22, 2007, A1.
[6] Heidy v. U.S. Customs Serv., 681 F. Supp. 1445, 1450-51 (C.D. Cal. 1988)
[7] *Id.* at 1453.
[8] *Id.* at 1452.

Law Caucus report being subject to elaborate secondary inspections each time they return to the United States, suggesting that an apparent match to the bloated watch list may be responsible. Some have even been told that the reason they were stopped is because they were "in the system" or because their name matched someone on a list.

Some travelers who are flagged by Customs because of the watch list may not in fact be on the list, but are misidentified with a watch listed person due to a similar name. Others may be on the list, but should not be: for instance, they may be listed because of false allegations or outdated information. Both categories of individuals -- those who are "misidentified" and those who are "mistakenly listed" -- end up suffering from the humiliation, stigma, anxiety, and inconvenience of repeated screenings at the border.

Customs and Border Protection screens individuals against more names on the spiraling terrorist watch list than any other agency, suggesting a particular need for congressional oversight of the agency's screening practices. Last fall, the General Accountability Office reported that the Terrorist Screening Database, the centralized terrorist watch list, had swollen from 150,000 records in June 2004 to 755,000 records in May 2007 – representing an alarming increase of 20,000 records per month.[9] This watch list is used by numerous agencies, including the Transportation Security Administration, the State Department, state and local police, and Customs and Border Protection; each agency uses a different subset of watch list records from the master list to screen individuals it encounters. But it is striking that Customs screens travelers against 98% of all records on the watch list[10] -- a higher percentage than any other federal agency – because it maintains the "least restrictive acceptance criteria" for including watch list records in its own screening database.[11]

The voluminous size of the watch list used by Customs to screen incoming travelers raises the question whether the agency is justified in choosing such minimal criteria for incorporating watch list records. Other agencies, such as the Transportation Security Administration, use a more selective subset of the watch list in part because the Department of Homeland Security believes that if a larger portion were used, "the number of misidentifications would increase to unjustifiable proportions."[12] The fact that Customs agents are screening travelers against nearly a million terrorist watch list records may be needlessly subjecting innocent individuals to invasions of privacy and civil liberties at U.S. borders.

Watch list accuracy and fairness

Recent government investigations suggest that the process for adding individuals, including U.S. citizens, to the watch list lacks adequate safeguards to ensure that only those who pose a real threat are included. First, a September 2007 Justice Department Inspector General audit of the watch list found enduring problems with the accuracy and quality of watch list records. For instance, the audit concluded that 38% of watch list records that had already been reviewed through the Terrorist

---

[9] GOV'T ACCOUNTABILITY OFFICE (GAO), TERRORIST WATCH LIST SCREENING: OPPORTUNITIES EXIST TO ENHANCE MANAGEMENT OVERSIGHT, REDUCE VULNERABILITIES IN AGENCY SCREENING PROCESSES, AND EXPAND USE OF THE LIST ("*GAO Opportunities*") 7-8 (Oct. 2007)

[10] Statement of Leonard Boyle before the House of Representatives Homeland Security Committee, 5, Nov. 8, 2007 *available online* at http://homeland.house.gov/SiteDocuments/20071108115249-02650.pdf.

[11] *GAO Opportunities*, *supra* note 9, at 32

[12] *GAO Opportunities*, *supra* note 9, at 36

Screening Center's routine "quality assurance" program contained errors or inconsistencies.[13] Furthermore, the Inspector General noted that nearly half of the records reviewed after individuals complained required changes or even removals from the list, suggesting "deficiencies" in the process for adding records to the watch list in the first place.[14]

Second, there is little independent review of the designation of individuals to the terrorist watch list, increasing the risk that innocent, law-abiding U.S. citizens and immigrants may be added to the list. A March 2008 Department of Justice Inspector General report found numerous problems with the submission of names to the watch list, leading to inaccurate and outdated data being included on the list.[15] The process for adding individuals to the list lacks rigorous review at any level. The Terrorist Screening Center (TSC), which maintains the list, does not vet the substance of nominations to the watch list, but merely accepts designations by other agencies.[16] Nor does the National Counterterrorism Center (NCTC), which is responsible for providing information to the TSC on individuals with possible ties to international terrorism.[17] The NCTC relies on designations from intelligence agencies such as the Federal Bureau of Investigation (FBI), but the Inspector General investigation found that FBI field offices were generally not reviewing nominations by individual field agents, bypassing an important level of review.[18]

The Inspector General found still other problems with the submission of names to the watch list. The NCTC had submitted names to the Terrorist Screening Center watch list based on FBI intelligence reports even when the FBI did not intend to nominate the individuals in question.[19] The FBI often failed to remove or modify watch list records, even after closing an investigation or receiving new information about an individual, and actually lacked procedures for the removal of certain classes of watch listed individuals.[20] The Inspector General report concluded that "the potential exists for the watchlist nominations to be inappropriate, inaccurate, or outdated because watchlist records are not appropriately generated, updated or removed as required by FBI policy."[21]

Racial profiling in watch list designations

Even more troubling, recent news reports state that the Attorney General is revising guidelines to permit the FBI to open investigations on individuals in the United States based on racial or religious profiling, and without any allegation of wrongdoing.[22] This development could directly lead to individuals being selected for border searches based on their race or religion, because subjects of even preliminary FBI investigations are generally added to the watch list[23], and individuals on the

[13] U.S. DEP'T OF JUSTICE OFFICE OF THE INSPECTOR GENERAL (OIG), FOLLOW-UP AUDIT OF THE TERRORIST SCREENING CENTER ("*2007 Follow-Up Audit*") iii (Sept. 2007)
[14] *Id.* at xix
[15] U.S. DEP'T OF JUSTICE OFFICE OF THE INSPECTOR GEN., AUDIT REPORT 08-16, AUDIT OF THE U.S. DEP'T OF JUSTICE TERRORIST WATCHLIST NOMINATION PROCESS ("*DOJ Nomination Process*"), (March 2008)
[16] U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., AUDIT REPORT 05-27, REVIEW OF THE TERRORIST SCREENING CENTER ("*DOJ 2005 Audit*"), 42 (2005).
[17] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, GAO-06-1031, "TERRORIST WATCH LIST SCREENING: EFFORTS TO HELP REDUCE ADVERSE EFFECTS ON THE PUBLIC ("*GAO Adverse Effects*"), 7 (Sept. 2007)
[18] *DOJ Nomination Process*, *supra* note 15, at 7-8
[19] *Id.* at 13-14
[20] *Id.* at 8-10
[21] *Id.* at 10
[22] Lara Jakes Jackson, *Proposed Rules Would Allow FBI to Use Profiles*, S.F. CHRON., July 3, 2008, A4.
[23] *GAO Opportunities*, *supra* note 9, at 22

watch list are flagged for intensive scrutiny at U.S. borders. Moreover, although the FBI is supposed to remove subjects of preliminary investigations from the watch list if the investigation fails to uncover wrongdoing, the March 2008 Inspector General audit showed that many individuals remain on the list even after investigations are closed. The prospect that U.S. citizens may be subject to invasive border searches and questioning based purely on a racial profile was deemed inappropriate and counterproductive *by every witness* at the Constitution subcommittee's recent hearing, yet appears likely to result from the Attorney General's revised guidelines.

Limited "redress" opportunities

While the Department of Homeland Security and other government agencies have created "redress" mechanisms for individuals who believe they are affected by government watch lists, U.S. citizens and residents who have used these processes often see no improvement in their experience. Many people who contacted the Asian Law Caucus had already filed complaints through the DHS "Traveler Redress Inquiry Program" (TRIP) or earlier versions of the redress program, or with U.S. Customs and Border Protection, but to no avail. One individual even reported retaliation for having complained to his congressional representative about repeated screenings; when he showed a Customs agent a supportive letter he had obtained from his representative, the questioning actually intensified. Others who contacted the Asian Law Caucus complained of excessive delays in getting any response from government agencies. Overall, individuals subject to repeated screenings continue to express a sense of powerlessness in resolving their predicament.

The fall 2007 GAO and Inspector General reports confirm that significant deficiencies exist in the redress procedures. The Inspector General found that, due in part to the absence of target time frames for completing redress requests, there were "excessive delays" in resolving complaints.[24] In addition, the same report noted that even where the Terrorist Screening Center revised its watch list in response to complaints, agencies relying on that data, including Customs, failed to update their records in a timely fashion[25] – perpetuating problems for travelers repeatedly screened at U.S. ports of entry. Finally, the Inspector General faulted the Terrorist Screening Center for lacking policies and procedures to *proactively* reduce watch list misidentifications, especially in light of the fact that almost half of the watch list encounters referred to the Center concerned individuals who were not on the list but merely shared a name that led to their misidentification.[26]

Government watch lists compiled by executive agencies in secrecy and without judicial determinations of guilt always burden the rights of those who are designated, since there is no adversarial, transparent process by which individuals named to the list can rebut derogatory allegations against them. But where, as here, the process for including individuals in a terrorist watch list provides even limited *internal* oversight—and may now explicitly allow for racial profiling—innocent Americans will almost certainly be unfairly targeted and deprived of their rights.

---

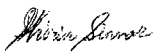
[24] *2007 Follow-Up Audit, supra* note 9, at iv, xix-xx, 45
[25] *Id.* at xx
[26] *Id.* at xxi

V. Conclusion

We urge the Constitution subcommittee to continue its investigation of Customs border searches and interrogations, including the First Amendment implications of agency practices and the intersection of Customs practices with the terrorist watch list. We encourage the subcommittee to request a GAO investigation on the impact of Customs policies on privacy and civil liberties and consider legislative and administrative reform to safeguard the rights of individuals returning to the United States.

Thank you for the opportunity to submit this statement. We would be pleased to work with the subcommittee further on this important issue, and can be reached at (415) 848-7714 or shirins@asianlawcaucus.org.

Sincerely yours,



Shirin Sinnar
Staff Attorney

U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and
Border Protection

JUL 3 0 2008

Shirin Sinnar, Staff Attorney
Asian Law Caucus
939 Market Street, Suite 201
San Francisco, CA 94103

Re: **FOIA Request H025725; Asian Law Caucus and the Electronic Frontier Foundation; CBP Policies and Procedures on Questioning and Searches**

Dear Ms. Sinnar:

This is the final response to your Freedom of Information Act (FOIA) request to U.S. Customs and Border Protection (CBP), dated October 31, 2007, seeking policies and procedures on: 1) the questioning of travelers and 2) inspections and searches of travelers' property.

By letter dated June 26, 2008, CBP provided you with an interim response consisting of 190 pages. An additional search of CBP headquarters and field offices for documents responsive to your request produced a total of 499 pages.

Of those 499 pages, I have determined that 184 pages of the records are releasable in their entirety; 287 pages are releasable in part with redactions pursuant to Title 5 U.S.C. § 552 (b)(2)(high), (b)(2)(low), (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E) (FOIA Exemptions 2(high), 2(low), 5, 6, b7(C) and b7(E)); and 28 pages have been withheld in their entirety pursuant to FOIA Exemptions 2(high), 2(low), 6, b7(C) and b(7)(E).

Enclosed are 471 pages with certain information withheld as described below.

FOIA Exemption 2 (high) protects information applicable to internal administrative and personnel matters, such as operating rules, guidelines, and manual of procedures of examiners or adjudicators, to the extent that disclosure would risk circumvention of an agency regulation or statute, impede the effectiveness of an agency's activities, or reveal sensitive information that may put the security and safety of an agency activity or employee at risk. Whether there is any public interest in disclosure is legally irrelevant. Rather, the concern under high 2 is that a FOIA disclosure should not benefit those attempting to violate the law and avoid detection.

FOIA Exemption 2(low) protects information applicable to internal administrative personnel matters to the extent that the information is of a relatively trivial nature and there is no public interest in the document.

FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The three most frequently invoked

privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege. After carefully reviewing the responsive documents, I determined that portions of the responsive documents qualify for protection under the

- **Deliberative Process Privilege**
  The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right privacy. The types of information that we have withheld consist of names of CBP personnel and other personal identification information. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

Exemption 7(C) protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. This exemption takes particular note of the strong interests of individuals, whether they are suspects, witnesses, or investigators, in not being unwarrantably associated with alleged criminal activity. That interest extends to persons who are not only the subjects of the investigation, but those who may have their privacy invaded by having their identities and information about them revealed in connection with an investigation. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, I have determined that the privacy interest in the identities of individuals in the records you have requested clearly outweighs any minimal public interest in disclosure of the information. Please note that any private interest you may have in that information does not factor into this determination. The types of information that we have withheld consist of names and other personal identification information.

Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. I determined that disclosure of information including law enforcement systems checks, locations and details regarding secure rooms, procedures relating to the supervision of detainees, procedures for the safeguarding of weapons, internal computer codes, list of items to be removed for an individual's safety, procedures regarding required approvals, procedures regarding internal coordination, techniques for identifying

potential terrorist suspects, special teams activated in response to certain incidents, details regarding questioning techniques, external coordination procedures and guidelines, information which would reveal the strengths and weaknesses of CBP programs, details regarding specific equipment used by CBP and specific step-by-step operational information could reasonably be expected to risk circumvention of the law. Additionally, the techniques and procedures at issue are not well known to the public.

Although I am aware that your request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you of your right to file an administrative appeal. If you are not satisfied with my action on your request, you may administratively appeal from this partial denial by writing to the FOIA Appeals Officer, Regulations and Rulings, Office of International Trade, U.S. Customs and Border Protection, 1300 Pennsylvania Ave., NW, Mint Annex, Washington, D.C. 20229, within sixty (60) days after the date of this determination letter. The appeal must be in writing and signed; contain your name and address; date of the initial request; date and control number of the letter denying your request; description of the records or information withheld; and reason(s) you believe that the records or information should be disclosed. Your appeal letter and mailing envelope should be marked "FOIA Appeal."

Sincerely,

Shari Suzuki, Chief
FOIA Appeals, Policy & Litigation Branch

Enclosure: Responsive Documents, 471 pages

000176

CUSTOMS DIRECTIVE

ORIGINATING OFFICE: FO:P

DISTRIBUTION: S-01
CUSTOMS DIRECTIVE NO. 3340-006A
DATE: FEBRUARY 4, 2000
SUPERSEDES: 3340-006, 6/12/86
REVIEW DATE: FEBRUARY 2002

SUBJECT: PROCEDURES FOR EXAMINING DOCUMENTS AND PAPERS

1 **PURPOSE.** This directive provides guidelines and procedures for examining documents and papers during all Customs operations at the border, functional equivalent of the border, and extended border.

2 **POLICY.**

2.1 The U.S. Customs Service will protect the rights of individuals against unreasonable search and seizure while still accomplishing its enforcement mission.

3 **AUTHORITIES/REFERENCES.** 19 C.F.R. 145.3; Ref. 3.740 LCCO; 19 U.S.C. 1305; National Stolen Property Act, 18 U.S.C. 2314; 18 U.S.C. 1426(h).

4 **EFFECTS ON OTHER DOCUMENTS.** The guidelines and procedures contained within this directive are currently contained within the Personal Search Handbook dated March 1997. These procedures will no longer be incorporated in the revised Personal Search Handbook HB #3300-04A dated November 1999.

5 **RESPONSIBILITIES.**

5.1 The Assistant Commissioner, Office of Field Operations, shall have policy oversight, which will include the formulation and implementation of guidelines and procedures.

5.2 The Assistant Commissioner, Office of Investigations, shall have oversight for investigative operations, which will include the implementation of guidelines and procedures set forth in this directive.

5.3 Special Agents in Charge (SAIC's) are responsible for ensuring that their subordinates get a copy of this directive and are familiar with its contents.

5.4 Directors, Field Operations, at Customs Management Centers are responsible for conducting ongoing reviews to evaluate procedures used for examining documents and papers.

5.5 Port Directors are required to update any necessary additional port-specific procedures for examining documents and papers and to ensure strict adherence to national policy.

000177

5.6 Each Customs officer must know the limits of Customs authority, and must use this authority judiciously, conscientiously, and courteously.

6 **PROCEDURES.**

6.1 All Customs officers shall comply with the following procedures.

6.2 **Customs Officers Should Not Read Personal Correspondence.**

6.2.1 The U.S. Customs Service must guard the rights of individuals being inspected to ensure that their personal privacy is protected. Therefore, as a general rule, Customs officers should not read personal correspondence contained in passengers' privately owned conveyances, baggage, or on their person, **except**, as specified in 6.4.1.

6.3 **Letter Class Mail.**

6.3.1 Customs officers may not read or permit others to read correspondence contained in sealed "LC" mail (the international equivalent of First Class) without an appropriate search warrant or consent.

6.3.2 Only articles presently in the postal system are deemed "mail." Letters carried by individuals, for example, are not considered to be mail, even if they are stamped (*see 19 C.F.R. 145.3*). [*Ref. 3.740 LCCO*].

6.4 **Customs Officers May Glance at Documents and Papers.**

6.4.1 As opposed to reading content, Customs officers may glance at documents and papers to see if they appear to be merchandise. This may include:

- Books, pamphlets, printed/manuscript material
- Monetary instruments.
- Prohibited materials such as, copyright violations, obscene, treasonous or seditious material (i.e., inciting or producing imminent lawless action).
- Prohibited matter being imported in violation of 19 U.S.C. 1305, stolen property under the National Stolen Property Act, 18 U.S.C. 2314, or evidence of embargo violations.
- Materials related to the importation or exportation of merchandise including documents required to be filed to import or export merchandise.

6.5 **Reasonable Suspicion Required for Reading and Continued Detention.**

6.5.1 If, after glancing at the documents or papers, an officer reasonably suspects that they relate to any of the categories listed in section 6.4.1 of this directive, the officer may read the documents. He/she may continue to detain such documents for such further inquiry as may be reasonably necessary to make the determination whether to seize the documents.

6.5.2 This may include referral to another agency necessary to assist in that determination.

6.6 **Probable Cause Required for Seizures.**

6.6.1 If an officer has probable cause to believe that a document or paper is subject to seizure because it is prohibited, a fruit, instrumentality or evidence of a crime, or otherwise subject to forfeiture, it may be seized.

6.7 **Probable Cause or Consent Required to Copy.**

6.7.1 An officer must have probable cause to believe a document or paper is subject to seizure, to copy it. Documents and papers may be copied without probable cause when consent to do so is obtained from the person from whom the documents were seized, or if copying is incident to a lawful arrest.

6.7.2 In circumstances when the inspecting Customs officer is uncertain whether probable cause exists, the officer may contact the Associate/Assistant Chief Counsel.

6.8 **Identification Documents can be Photocopied.**

6.8.1 Passports (United States or foreign), Seaman's Papers, Airman Certificates, drivers licenses, state identification cards and similar governmental identification documents can be photocopied for legitimate, good-faith government purposes without any suspicion of illegality.

6.8.2 Certificates of Naturalization may never be copied (18 U.S.C. 1426(h)).

6.9 **Attorney-Client Privilege.**

6.9.1 As part of a border search, an attorney's files can be examined for the presence of drugs, currency or other monetary instruments, sales slips, invoices, or other documents evidencing foreign purchases.

6.9.2 Occasionally, an attorney will claim that the attorney-client privilege prevents the search of his documents and papers at the border. Files and papers being brought into the country by an attorney are subject to a routine search for merchandise. Implicit in the authority to search for merchandise is the authority to search for papers that indicate or establish that a current importation of merchandise might be occurring. Records of an importation are not privileged. However, correspondence, court papers, and other legal documents may be privileged. If an officer has probable cause to believe a document may be evidence of a crime, seek advice from the Associate/Assistant Chief Counsel or the U.S. Attorney's office.

6.10 **Chain of Custody Required for Copies.**

6.10.1 Whenever copies of documents are made, transfer of the copies should be accomplished through a chain of custody form (CF-6051) or other documentation that will show each individual who has had custody and access to such copies.

6.11 **Foreign Language Documents or Documents Requiring Special Expertise.**

6.11.1 If an officer reasonably suspects that a document or paper in a foreign language falls into a category that would allow it to be read, the document can be detained and forwarded to an appropriate translator, provided that such translations can be accomplished within a reasonable time.

6.11.2 The use of a facsimile (FAX) machine, when appropriate, is authorized. This same principle would apply to documents that need special expertise to determine their nature, such as documents relating to complex technology cases.

6.11.3 If after translation or review, probable cause to seize develops, the documents should be seized and/or copies retained. If not, the originals must be returned and all copies (e.g., fax) must be destroyed. The destruction must be appropriately documented.

6.11.4 Factors that a court might consider in determining the reasonableness of the time the documents are detained could be such things as the nature of the documents, whether the officer explained to the person the reason for the detention, and whether the person was given the option of continuing his journey with the understanding that Customs would return the documents if it is not in violation of law.

7 **MEASUREMENT.** Directors, Field Operations, at Customs Management Centers, SAIC's, and Port Directors will ensure that all TECS reports pertaining to the examinations of documents and papers are reviewed periodically to determine the effectiveness of the procedures contained within this directive, including whether there may be any improprieties in the conduct of these examinations.

8 **NO PRIVATE RIGHT CREATED.** This document is an internal policy statement of the U.S. Customs Service and does not create any rights, privileges, or benefits for any person or party.

Commissioner of Customs

U.S. Customs and Border Protection

Policy Regarding Border Search of Information

July 16, 2008

This policy provides guidance to U.S Customs and Border Protection (CBP) Officers, Border Patrol Agents, Air and Marine Agents, Internal Affairs Agents, and any other official of CBP authorized to conduct border searches (for purposes of this policy, all such officers and agents are hereinafter referred to as "officers") regarding the border search of information contained in documents and electronic devices. More specifically, this policy sets forth the legal and policy guidelines within which officers may search, review, retain, and share certain information possessed by individuals who are encountered by CBP at the border, functional equivalent of the border, or extended border. This policy governs border search authority only; nothing in this policy limits the authority of CBP to act pursuant to other authorities such as a warrant or a search incident to arrest.

A. Purpose

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 material, 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 are essential to uncovering vital law enforcement information. For example, examinations of documents and electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography, monetary instruments, and information in violation of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

Notwithstanding this law enforcement mission, in the course of every border search, CBP will protect the rights of individuals against unreasonable search and seizure. Each operational office will maintain appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this policy.

B. Review of Information in the Course of Border Search

Border searches must be performed by an officer or otherwise properly authorized officer with border search authority, such as an ICE Special Agent. In the course of a border search, and absent individualized suspicion, officers can review and analyze the information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States, subject to the requirements and limitations provided herein. Nothing in this policy limits the authority of an officer to make written notes or reports or to document impressions relating to a border encounter.

C. Detention and Review in Continuation of Border Search

(1) Detention and Review by Officers. Officers may detain documents and electronic devices, or copies thereof, for a reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location. Except as noted in section D below, if after reviewing the information there is not probable cause to seize it, any copies of the information must be destroyed. All actions surrounding the detention will be documented by the officer and certified by the Supervisor.

(2) Assistance by Other Federal Agencies or Entities.

(a) Translation and Decryption. Officers may encounter information in documents or electronic devices that is in a foreign language and/or encrypted. To assist CBP in determining the meaning of such information, CBP may seek translation and/or decryption assistance from other Federal agencies or entities. Officers may seek such assistance absent individualized suspicion. Requests for translation and decryption assistance shall be documented.

(b) Subject Matter Assistance. Officers may encounter information in documents or electronic devices that is not in a foreign language or encrypted, but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by CBP. With supervisory approval, officers may create and transmit a copy of information to an agency or entity for the purpose of obtaining subject matter assistance when they have reasonable suspicion of activities in violation of the laws enforced by CBP. Requests for subject matter assistance shall be documented.

(c) Original documents and devices should only be transmitted when necessary to render the requested assistance.

(d) Responses and Time for Assistance.

(1) Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include any findings, observations, and conclusions relating to the laws enforced by CBP.

(2) Time for Assistance. Responses from assisting agencies are expected in an expeditious manner so that CBP may complete its border search in a reasonable period of time. Unless otherwise approved by the principal field official such as the Director, Field

Operations or Chief Patrol Agent, responses should be received within fifteen (15) days. This timeframe is to be explained in the request for assistance. If the assisting agency is unable to respond in that period of time, CBP may permit extensions in increments of seven (7) days. For purposes of this provision, ICE is not considered to be a separate agency.

(e) Destruction. Except as noted in section D below, if after reviewing information, probable cause to seize the information does not exist, any copies of the information must be destroyed.

D. Retention and Sharing of Information Found in Border Searches

(1) By CBP.

(a) 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—they may seize and retain the originals and/or copies of relevant documents or devices, as authorized by law.

(b) Other Circumstances. Absent probable cause, CBP may only retain documents relating to immigration matters, consistent with the privacy and data protection standards of the system in which such information is retained.

(c) Sharing. Copies of documents or devices, or portions thereof, which are retained in accordance with this section, may be shared by CBP with Federal, state, local, and foreign law enforcement agencies only to the extent consistent with applicable law and policy.

(d) Destruction. Except as noted in this section, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

(2) By Assisting Agencies and Entities.

(a) During Assistance. All documents and devices, whether originals or copies, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to CBP.

(b) Return or Destruction. At the conclusion of the requested assistance, all information must be returned to CBP as expeditiously as possible. In addition, the assisting Federal agency or entity must certify to CBP that all

copies of the information transferred to that agency or entity have been destroyed, or advise CBP in accordance with section 2(c) below.

(i) In the event that any original documents or devices are transmitted, they must not be destroyed; they are to be returned to CBP unless seized based on probable cause by the assisting agency.

(c) Retention with Independent Authority. Copies may be retained by an assisting Federal agency or entity 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 of its decision to retain information on its own authority.

E. Review and Handling of Certain Types of Information

(1) Business Information. Officers encountering business or commercial information in documents and electronic devices shall treat such information as business confidential information and shall take all reasonable measures to protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may govern or restrict the handling of the information.

(2) Sealed Letter Class Mail. Officers may not read or permit others to read correspondence contained in sealed letter class mail (the international equivalent of First Class) without an appropriate search warrant or consent. Only articles in the postal system are deemed "mail." Letters carried by individuals or private carriers such as DHL, UPS, or Federal Express, for example, are not considered to be mail, even if they are stamped, and thus are subject to a border search as provided in this policy.

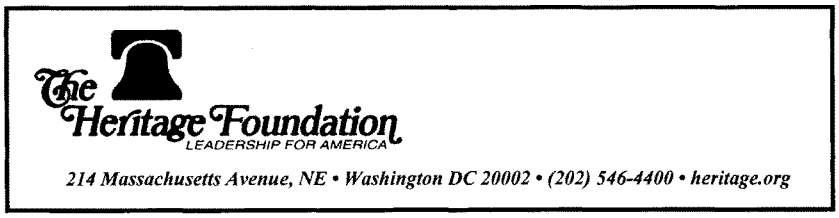
(3) Attorney-Client Privileged Material. Occasionally, an individual claims that the attorney-client privilege prevents the search of his or her information at the border. Although legal materials are not necessarily exempt from a border search, they may be subject to special handling procedures.

Correspondence, court documents, and other legal documents may be covered by attorney-client privilege. If an 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 officer must seek advice from the Associate/Assistant Chief Counsel or the appropriate U.S. Attorney's office before conducting a search of the document.

(4) Identification Documents. Passports, Seaman's Papers, Airman Certificates, driver's licenses, state identification cards, and similar government identification documents can be copied for legitimate government purposes without any suspicion of illegality.

F. No Private Right Created

This document is an internal policy statement of CBP and does not create any rights, privileges, or benefits for any person or party.



CONGRESSIONAL TESTIMONY

Border Inspection "Search" Strategies: Managing Risk and Focusing Resources

Testimony before
Committee on the Judiciary
United States Senate

June 25, 2008

James Jay Carafano, Ph.D.

My name is James Jay Carafano. I am the Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and a Senior Research Fellow for the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation. The views I express in this testimony are my own, and should not be construed as representing any official position of The Heritage Foundation.

Mr. Chairman and other distinguished Members, thank you for the opportunity to testify before you today. In my testimony, I would like to (1) make the case that the public policy issues regarding searches and inspections at border ports of entry and exit (including searching electronic equipment, such as computers and personal digital devices) are more important than the narrow legal issues, (2) explain why searches are an important component of effective border security strategy and advocate for continuing to allow federal entities broad discretionary authority in implementing the searches and inspections at the border, and (3) offer some specific proposals on ensuring that border searches and inspections remain an efficient and effective component of border security strategy.

A War to Be Won

It should be acknowledged at the outset that there is clearly a need for effective searches and inspections at US ports of entry. Hundreds of millions of people cross the U.S. border each year in numbers approaching twice the population of the United States. The overwhelming majority travel through legal points of entry and exit, such as land border crossing points, airports, and harbors. Billions of tons of goods, accounting for a third of the U.S. gross domestic product, transit America's borders as well. Terrorists and transnational criminals have attempted to exploit every known *legal* means for moving people, goods, and services across U.S. borders. In fact, virtually every known or suspected terrorist has exploited legal opportunities to enter or remain in the United States. Most passed through screening at an established point of entry.

These vulnerabilities make it likely that terrorists will continue to use sophisticated travel methods to enter the United States, including acquiring new passports to hide past travel. They will do this because there is still no viable, reliable means of ensuring that important information on terrorist travel gets to frontline officers.

Effective security at the points of entry and exit is essential not only to keeping bad things and bad people out of the United States, but also to protecting the border crossing cites-- key nodes in the networks that connect America to the world of global commerce. This security has to be provided while facilitating the free flow of goods, people, services, and ideas that are the lifeblood of the American economy and a key competitive advantage for the United States in the worldwide marketplace.

As the 9/11 Commission rightly noted, "The challenge for national security in an age of terrorism is to prevent the very few people who may pose overwhelming risks from entering or remaining in the United States undetected." The most vital national security

mission for U.S. border assets is to identify high-risk people and cargo entering the United States and take appropriate action.

Terrorist threats aside, there are numerous other criminal and malicious activities that routinely seek to exploit the relative freedom of traversing US borders. There is a rampant problem of drug, weapons, and human trafficking which occur at our borders.

Thus, there is little question that searches and inspections are vital to US safety, prosperity, and security.

A Question of Policy

Many of the criticisms aimed at the government, and specifically the Custom and Border Protection, have claimed that intrusive border searches, including inspecting computers and other electronic devises, are illegitimate and unconstitutional. This practice of misusing or reinterpreting laws to make American actions appear illegitimate is called "lawfare," instead of debating whether or not this is a useful, practical and acceptable practice for the sake of national security.[1] Federal authorities have an unquestionable right to conduct legitimate searches at ports of entry. The Ninth Circuit and Fourth Circuit courts agree that searching laptops at the border is legal. The concerns of privacy and civil liberties are always important. However, at this point finding ways to prove that the Department of Homeland security is somehow conducting illegal searches is not prudent. Instead, we should be discussing if the policy is right or wrong and what we must do to make it better.

Enforcing Laws at the Border

Customs and Border Patrol agents have a difficult mission. At the border, these CBP agents must determine in a matter of minutes if persons represent a concern for public safety or security. They must do this in a manner that is (1) appropriate under US law, (2) does not unnecessarily impede legitimate trade and travel, and (3) safeguards US interests. In addition, CBP agents are also responsible for enforcing our customs laws. They are charged with preventing a variety of things from entering this country from fruits, pirated goods, and child pornography to explosives and biological weapons.

In this regard, searches of laptops and other electronic equipment is not unreasonable. Electronic equipment can and has been used to carry illicit goods and information. There are numerous examples where border agents have found laptops contained files reflecting illegal activity. One such example would be the case of Michael Arnold who had his laptop searched in 2005, leading agents to find child pornographic pictures and arrest him.[2]

---

[1] Lee A. Casey and David B. Rivkin, Jr., "International Law and the Nation-State at the U.N.: A Guide for U.S. Policymakers," Heritage Foundation *Backgrounder* No. 1961, August 18, 2006, at www.heritage.org/Research/WorldwideFreedom/bg1961.cfm.

[2] Gautham Nagesh, "Groups ask court to reverse ruling, limit laptop searches at border," *NextGov*, June 13, 2008, at http://www.nextgov.com/nextgov/ng_20080613_2643.php (June 19, 2008).

Nor are electronics exclusive of our enemies. Analysts have documented, for example, a steady increase in terrorists' use of the Internet.[3] Searching laptops serve as an important layer for DHS's counter-terrorism efforts. There have been numerous instances where information gathered from terrorist laptops has provided crucial information.

Discretionary Authority

CBP must be able to adapt to threats for which our enemies will constantly be seeking new tactics to elude them. In order to be successful, CBP must avoid predictable patterns of behavior. We should retain the tradition of discretion of law enforcement officers to apply their judgment to when searches are appropriate.

This ability for CBP agents was crucial in stopping the millennium bomber. In 1999, CBP agents elected to search Ahmed Ressam's vehicle due to suspicious behavior while answering usual questions at the border. The ability for agents to act on their suspicions led them to discover explosives in Ressam's trunk. [4]

Responsible Implementation

The public policy debates about security and civil liberties are often framed in a zero sum context—where any advance in national security policies necessarily comes at the expense of civil liberties. In practice, however, good public policies equally advance the causes of enhancing public safety and security and protecting individual liberties.

It is important that we take into consideration concerns over privacy when conducting searches on an individual's laptop, and thus this practice should be done in a responsible manner. The best strategy to secure this country is a layered and risk-based approach.

The Department of Homeland Security should

- **Effectively employ intelligence and information sharing to better target border searches.** CBP must work closely with Immigration and Customs Enforcement and other federal law enforcement agencies, as well as state and local law enforcement partners to identify high risk travelers and target searches more effectively. Connecting the dots, making sure that the right information gets to the right person in order to do the right thing, is the single greatest capability needed to integrate international, border, and internal enforcement. DHS lacks an integrated intelligence plan and mechanisms to distribute information effectively. A more concerted intelligence effort is required.

---

[3] For example, see Jim Melnick, "The Cyberwar Against the United States," *The Boston Globe*, August 19, 2007, at www.boston.com/news/globe/editorial_opinion/oped/articles/2007/08/19/the_cyberwar_against_the_united_states (January 31, 2008).

[4] "Millenium Bomber' sentenced to 22 years for bomb plot," *U.S. Customs and Border Protection Today*, Vol. 3, Nos. 7/8 (July/August 2005), at *http://www.cbp.gov/xp/CustomsToday/2005/Jul_Aug/other/ahmed_ressam.xml* (June 20, 2008).

DHS should make development of an integrated plan for intelligence, surveillance, and reconnaissance for border and internal enforcement a top priority. The department should work with the Director of National Intelligence to better leverage other capabilities of the intelligence community (such as those of the CIA and the Pentagon) in support of border operations.

- **Obtain traveler information earlier.** Continuing to push the border outward is a smart strategy. A new program DHS is launching for travelers from visa-waiver countries called Electronic System for Travel Authorization (ESTA) allows travelers to enter in information online prior to departure. ESTA will be used to replace the paper based forms travelers must complete while on the airplane. That coupled with initiatives like checking flight manifests, allow CBP agents more time to examine information, and will greatly enhance their ability to target the real threats. ESTA should be improved to ensure full participation by making it available for all potential users, that is providing the application in other languages and in non web-based form. In addition, DHS should have a grievance procedure that provides information for denied applicants.[5]
- **Conduct searches based on a risk-based assessments.** By taking a targeted approach, CBP agents can focus their time and resources on those they identify as posing a risk. A vast majority of travelers do not proceed to secondary screenings, however, those who require it could have their laptops searched if needed.
- **Improve human capital and continuous technology.** Continue to emphasize training of one face at the border so that they have skills to do effective risk assessments and deploy technologies so they have the information they need to do this better. At the Nogales port of entry, CBP is testing an advanced computerized screening system that checks people as they cross the border. The real value of these systems is not checking and scrutinizing every individual, rather it is looking for anomalies and patterns that allow border enforcement to target criminal smuggling gangs. The technologies being tested at Nogales speed up legitimate trade and travel and allow border enforcement at the ports of entry to focus criminal activity.

Conclusion

It is not reasonable to ignore the potential threats that come with laptops. Conducting searches in responsible manners helps protect the American public in a respectful manner. Thank you for the opportunity to discuss this important issue and I look forward to your questions.

****

[5] Jena Baker McNeill, "Electronic Travel Authorization: Important for Safe and More Secure Overseas Travel," Heritage Foundation *WebMemo* No. 1964, June 19, 2008, at *http://www.heritage.org/Research/HomelandSecurity/wm1964.cfm.*

The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2007, it had nearly 330,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2007 income came from the following sources:

Individuals	46%
Foundations	22%
Corporations	3%
Investment Income	28%
Publication Sales and Other	0%

The top five corporate givers provided The Heritage Foundation with 1.8% of its 2007 income. The Heritage Foundation's books are audited annually by the national accounting firm of McGladrey & Pullen. A list of major donors is available from The Heritage Foundation upon request.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON THE CONSTITUTION

Hearing on
"Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel"

June 25, 2008
9:00 A.M.
Dirksen Senate Office Building, Room 226

Testimony of

LARRY CUNNINGHAM

Until June 30, 2008
Assistant District Attorney
Bronx District Attorney's Office
Bronx, New York

Effective July 1, 2008
Assistant Professor of Legal Writing
St. John's University School of Law
Jamaica, New York

Telephone (212) 920-4623
E-mail larry.cunningham@yahoo.com

TABLE OF CONTENTS

Chairman Feingold, Senator Brownback, and Members of the Subcommittee on the Constitution:

Introduction

Thank you for inviting me to testify about about this important topic. My name is Larry Cunningham. I am, until next Monday, an Assistant District Attorney in the Appeals Bureau of the Bronx County District Attorney's Office in New York City.[1] Beginning next Tuesday, I will be a professor at St. John's University School of Law in Queens, New York, where I will be teaching legal writing. My experience with the topic of border searches stems from my research into this area while I was a law professor in Texas. I subsequently published an article analyzing the law of border searches in the Quinnipiac Law Review, volume 26, page 1. I have also taught the law of search and seizure as both a full-time and adjunct law professor.

Before directly addressing the topic that is the subject of today's hearing, I would like to make four observations. *First*, I understand the term "laptop search" to mean an investigation into the electronic contents of a laptop computer—the files and information that are contained in the computer's hard drive or its memory. By this, I understand to *exclude* from its definition the physical search of the compartments of the laptop itself. In other words, outside the scope of today's discussion would be the search for narcotics or other contraband secreted in, say, a CD or DVD drive. Today's hearing, as I understand it, concerns the permissibility of a government agent's search of the electronic information contained in a laptop computer at the border.

Second, the relevant question is not whether a person feels that his privacy has been intruded upon when a customs agent searches his laptop. All government searches will, by definition, involve some intrusion into a person's subjective expectation of privacy. Otherwise,

[1] I am speaking today in my individual capacity; my views do not necessarily reflect those of the District Attorney.

they would not be considered "searches" for purposes of the Fourth Amendment. In *Katz v. United States*,[2] the Supreme Court held that whether there is a "search" at all, for Fourth Amendment purposes, depends on an affirmative answer to the threshold question: Has there been a breach of the reasonable expectation of privacy?

Third, the Constitution's text does not prohibit the government from conducting searches that intrude into people's privacy. What the text of the Fourth Amendment *does* prohibit is the conducting of *unreasonable* searches or seizures. Conversely, then, the Fourth Amendment permits *reasonable* searches and seizures. Through over two hundred years of case law, the Supreme Court has tried to define the boundaries between "reasonable" and "unreasonable" searches and seizures.

Fourth, then, we know that the extent of the privacy intrusion is only the beginning step of a constitutional or policy inquiry into a particular search or seizure practice. The discussion must then consider the reasonableness, or unreasonableness, of the practice. The Supreme Court has said that reasonableness, in turn, requires a balancing between the relevant government interests, on the one hand, and the privacy interests at stake, on the other.

With these preliminary considerations and observations in mind, I will now turn to the question of laptop searches at the border. I will do so by discussing, first, the background of border searches in order to provide historical context for the topic. Second, I will address the current state of the law dealing with border searches, in general, and laptops, in particular. Third, I will analyze the relevant policy considerations to determine whether some oversight or

---

[2] 389 U.S. 347 (1967).

legislative action is necessary. Fourth, I will offer some modest proposals for legislative action or administrative regulation.

I. The Historical Background of Border Searches

In assessing "reasonableness," the modern Supreme Court starts with the general proposition that, ordinarily, searches and seizures must be preceded by a warrant and a judicially-determined finding of probable cause, "subject only to a few specifically established and well-delineated exceptions."[3] Among those exceptions is the "border search exception," which permits the search of persons or property crossing the international border without a warrant or probable cause.

The Supreme Court did not officially and directly recognize this exception until 1977. Prior to that, it had hinted—through *dicta* in several cases—that such an exception existed. In *Boyd v. United States*, a civil forfeiture case from 1886, the Supreme Court had to decide whether customs agents lawfully seized several plates of glass, alleged to have been illegally imported by the claimant. At issue was the seizure of the goods, not the search that led to them. The Supreme Court upheld the seizure under the Fourth Amendment, noting that the seizure of contraband had been authorized at common law, by English statute, and by the First Congress—the same body that went on to propose the Fourth Amendment to the states several months later. This latter, historical argument is significant because the same statute that authorized the seizure of contraband also authorized the warrantless search of ships and vessels for goods subject to duty. Therefore, an extension of the *Boyd* Court's reasoning would support the border search exception. If that Court upheld one aspect of the statute (the provision permitting seizure) then it

[3] *Id.* at 357.

stands to reason that the rest of the statute (authorizing warrantless searches) was also constitutional.

The Supreme Court also alluded to a border search exception in *Carroll v. United States*, the case that recognized the car search exception, which permits the warrantless search of an automobile, provided the police have probable cause to believe that evidence or contraband is contained in the vehicle. In *Carroll*, Chief Justice Taft cited *Boyd* for the proposition that there is a fundamental difference between a search of a person's home and the search of goods that are in the "course of transportation."[4] When contraband goods are in transit, "it is not practicable to secure a warrant, because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought."[5] Having established that the warrant requirement did not apply to car searches, the Court next addressed under what circumstances such stops could occur. The Court rejected a rule that would authorize the stop of every car on a road in the hope that contraband might be uncovered.[6] Such blanket and suspicionless searches violated the Constitution, Taft held.[7] The Court made a point of drawing a distinction to border searches, however. The Court noted:

> Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.[8]

---

[4] *Id.* at 151, 153.

[5] *Id.* at 153.

[6] *Id.* at 154.

[7] *Id.*

[8] *Id.* at 153-54.

While *dicta*, this passage was strong support for the belief that, at least in 1925 when *Carroll* was decided, the suspicionless and warrantless searches of persons at the border were considered reasonable.

The Supreme Court continued alluding to a border search exception in *dicta* in two obscenity cases in the early 1970s. In *United States v. Thirty-Seven (37) Photographs*,[9] the claimant returned to the United States from a trip to Europe with several pictures from the *Kama Sutra*, which he intended to sell. Customs officials seized the photographs under a statute prohibiting the importation of obscene materials. The Supreme Court construed the statute to require a prompt determination, by a judge, of whether the seized items were in fact obscene. The Court rejected a First Amendment challenge to the statute, holding that Congress had the power to prohibit the importation of goods, even if the possession and viewing of the items within the privacy of one's home, could not subject the claimant to prosecution. The Court reasoned that a port of entry is markedly different from the private sanctum of a person's home. The Court stated:

> [A] port of entry is not a traveler's home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search. *Customs officers characteristically inspect luggage and their power to do so is not questioned in this case; it is an old practice and is intimately associated with excluding illegal articles from the country.*[10]

The Court concluded that Congress may constitutionally prohibit the importation of obscene materials.[11]

---

[9] 402 U.S. 363 (1971).

[10] *Id.* at 376 (emphasis added).

[11] *Id.*

In *United States v. 12,200-Ft. Reels of Super 8mm. Film*,[12] the Supreme Court applied the holding of *Thirty-Seven Photographs* to an end-user who had imported pornographic films for his private use. The Court, as in *Thirty-Seven Photographs*, relied on its conception of the international border as being constitutionally different from the interior of the country. The Court wrote:

> Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations.[13]

The Court noted that the text of the Constitution[14] gives broad power to Congress to regulate international commerce. "Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry."[15]

In *Almeida-Sanchez v. United States*,[16] the Court came closest to addressing the constitutionality of border searches. The defendant was stopped by a "roving patrol" of the United States Border Patrol. He was stopped on a state highway in California, traveling on an east-west highway that was 25 air miles north of the Mexican border.[17] Citing *Boyd* and *Carroll*, the Court in *dicta* upheld routine border searches. The Court wrote:

> It is undoubtedly within the power of the Federal Government to exclude aliens from the country. ... It is also without doubt that

---

[12] 413 U.S. 123 (1973).

[13] *Id.* at 125.

[14] U.S. CONST. art. I, § 8, cl. 3.

[15] *12,200-Ft. Reels of Super 8mm. Film*, 413 U.S. at 125.

[16] Almeida-Sanchez v. United States, 413 U.S. 266 (1973).

[17] *Id.* at 267-69.

> this power can be effectuated by routine inspections and searches of individuals or conveyances seeking to cross our borders.[18]

The Court also opined that a routine border search would also be permissible at the "functional equivalent" of the border, such as fixed checkpoints in the interior of the country or at airports where an international flight makes its first stop in the country.[19] However, the Court declined to extend this principle to the roving patrol at issue in the case. Describing the search as "of a wholly different sort," the Court held that suspicionless searches in the interior of the country were unconstitutional, citing *Carroll*.[20]

The Supreme Court directly confronted the issue of the constitutionality of warrantless and suspicionless border searches in *United States v. Ramsey*.[21] The defendants were convicted of, among other things, the illegal importation of heroin. The defendants ran a heroin-by-mail enterprise in which they sent heroin from Thailand through the international mail to co-conspirators in the United States, who would then distribute the drugs domestically. A customs inspector, on-duty at the sorting facility of the New York Post Office, noticed that there were several bulky envelopes that had been mailed from Thailand. He felt the envelopes and concluded that they contained something other than letters. He opened them and found heroin. Writing for a 5-4 majority, then-Justice Rehnquist upheld the search. The Court first put to bed the question of whether border searches, in general, are constitutional without a warrant or suspicion:

---

[18] *Id.*

[19] *Id.* at 272-73.

[20] *Id.* at 274-75.

[21] 431 U.S. 606 (1977).

> 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, should, by now, require no extended demonstration.[22]

In support, the Court looked principally to history. The Court re-adopted *Boyd*'s historical argument. The Congress that proposed the Bill of Rights had, only a few months earlier, enacted a customs statute that permitted the warrantless search of "any ship or vessel, in which [customs officers had] reason to suspect any goods, wares or merchandise subject to duty [were] concealed."[23] In contrast, the search of homes, stores, and other buildings required a warrant.[24] The Court cited *Carroll*, *Thirty-Seven Photographs*, *12,200-Ft. Reels of Film*, and *Almeida-Sanchez* for the proposition that there was a consistent and long history of support for the border search exception.

The Court also viewed the border as having a talismanic significance. The Court wrote:

> Border searches, then, from before the adoption of the Fourth Amendment, have been considered to be "reasonable" *by the single fact that the person or item in question has entered into our country from outside*.[25]

This passage suggests that the Court viewed the border as having a special significance under Fourth Amendment, not unlike the car, home, or school. While the Court has repeated *Katz*'s warning that the Fourth Amendment protects "people, not places,"[26] one cannot help but read *Ramsey* as holding that the border is an area in which special Fourth Amendment rules apply.

---

[22] *Id.* at 616.

[23] *Id.* (quoting 1 Stat. 29, § 24).

[24] *Id.*

[25] *Id.* at 619 (emphasis added).

[26] *Katz*, 389 U.S. at 349.

Later, the Court talked about the border search exception as being grounded in a "right" of the government to control the entry of persons and objects into the country.[27] The Court did not expand upon its rationale, except to note later in the opinion that "the 'border search' exception is not based on the doctrine of 'exigent circumstances' at all."[28]

The question for the Court was whether the search fell within or without the general exception. The defendant conceded, at oral argument, that Customs could open an envelope hand-carried by a passenger walking across the border. The question, then, was whether the mode of an object's entry should make a difference. The Court concluded that the "critical fact" was the border crossing, not the manner in which it was made.[29] The Court also rejected the defendant's First Amendment arguments. Here, the Court relied on a diminished expectation of privacy at the border: "There are limited justifiable expectations of privacy for incoming material crossing United States borders."[30] Specifically, the defendant was unable to demonstrate why a letter that is mailed should possess a greater expectation of privacy than a letter that is hand-carried across the border.

II. The Law

In light of *Ramsey*, the present state of the law is this: Persons and property entering the United States from abroad are subject to warrantless and suspicionless search. Routine searches at the border are justified, under the Constitution, for the following reasons:

---

[27] *Ramsey*, 431 U.S. at 620. ("The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country.").

[28] *Id.*

[29] *Id.* at 620.

[30] *Id.* at 623 n.17.

- historically, customs and border officials have had broad latitude to conduct suspicionless and warrantless searches at the border or its functional equivalent;
- the sovereign has an inherent right to control who and what crosses its borders;
- searches are necessary to protect the interior from contraband and disease; *and*
- there is a diminished expectation of privacy at the border.

The border search exception comes with an important caveat, however. A suspicionless and warrantless search is permitted only for so-called "routine" searches, such as opening a piece of mail or patting down a person crossing the border. "Non-routine" border searches require something more, the Supreme Court held in *United States v. Montoya de Hernandez*.[31]

Rosa Elvira Montoya de Hernandez arrived at Los Angeles International Airport on a flight from Bogota, Colombia. A customs inspectors grew suspicious because she had made a number of recent trips to Miami and Los Angeles, had no friends in the United States, did not have hotel reservations, had $5,000 in cash but no billfold, could not recall how she purchased the plane ticket, and had a suspicious story about coming to the United States to buy supplies for her husband's store. A female inspector was summoned to pat-down the defendant. The pat-down revealed that the defendant's abdomen felt firm and full. The inspectors accused the defendant of being an "alimentary canal smuggler"—one who swallows balloons or condoms filled with drugs, crosses the border, and then excretes the packages and delivers them to an

[31] 473 U.S. 531 (1985).

awaiting drug dealer. The inspectors asked the defendant for permission to x-ray her, which the defendant agreed to. The defendant stated she was pregnant, so the inspectors said they would give her a pregnancy test. The defendant withdrew consent after she learned that the inspectors would handcuff her on the ride to the hospital. The inspectors then offered her a choice: submit to an x-ray, wait in the customs area until she produced a monitored bowel movement, or return to Colombia. The defendant chose the last option, but the inspectors were unable to arrange a direct flight to Bogota. The defendant was placed in an empty office with a wastebasket. She was informed that if she had to go to the bathroom, she would have to use the wastebasket. The defendant was confined in the room for approximately 16 hours, most of the time spent curled up on a chair. She refused all offers of food and drink. After 16 hours, customs sought and obtained a court order authorizing a pregnancy test, x-ray, and rectal exam. The defendant was taken to a hospital where a physician performed a rectal exam. The doctor removed a balloon with drugs. Over the next several days, the defendant excreted 88 balloons containing 528 grams of cocaine.

At issue was the 16-hour detention and seizure of the defendant. The defendant claimed that this was an unreasonable seizure and hence the subsequent search was invalid. Writing for the majority, then-Justice Rehnquist noted first the context of the seizure:

> Here the seizure of respondent took place at the international border. Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country. ... This Court has long recognized Congress' power to police entrants at the border.[32]

[32] *Id.* at 537.

Congress has a legitimate concern about the "integrity of the border," a concern only heightened by what Rehnquist called the "veritable national crisis in law enforcement caused by smuggling of illicit narcotics ... and in particular by the increasing utilization of alimentary canal smuggling."[33] Because the government's interests in protecting the border are so strong, the "Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior."[34] In contrast, the defendant's expectation of privacy was less at the border because she had requested to be admitted to the country and had subjected herself to the laws of the United States.[35] The Court concluded that the balancing of the interests of the government and the individual "is ... struck much more favorable to the Government at the border."[36]

But the Court noted that *Ramsey* concerned itself with a routine border search, and that the Court had never decided what was required for a non-routine search or seizure at the border.[37] The Court rejected the Ninth Circuit's test, which would have permitted the detention of an entrant only upon "clear indication" of alimentary canal smuggling.[38] The Court looked instead to the familiar Fourth Amendment standard of "reasonable suspicion:"

> We hold that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding

---

[33] *Id.* at 538.

[34] *Id.*

[35] *Id.* at 539 (citing *Carroll v. United States*, 267 U.S. 132 [1925] and 19 U.S.C. § 482).

[36] *Id.* at 540.

[37] *Id.*

[38] *Id.* at 540-41.

> the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal.[39]

The Court upheld the detention of Montoya de Hernandez because the inspectors had reasonable suspicion that the defendant had drugs in her alimentary canal. The inspectors had more than a hunch. The circumstances of the defendant's entry into the country were suspicious, and the defendant did not help her case with her implausible story. This justified the inspectors' initial detention of the defendant. The continued detention (for over 16 hours) was justified because of the unique nature of alimentary canal smuggling. It is difficult to confirm whether a person is an alimentary canal smuggler because of the nature of the biological processes involved. Unlike brief *Terry*-like encounters,[40] this type of drug smuggling cannot be detected in a matter of moments. The inspectors reasonably expected that Montoya de Hernandez's detention would be brief because she had not gone to the bathroom in quite some time. The detention lasted so long because the defendant chose to "resist the call of nature."[41] "[Montoya de Hernandez] alone was responsible for much of the duration and discomfort of the seizure."[42]

Justice Brennan dissented, arguing that the customs officials needed both probable cause and a warrant in order to detain the defendant for so long. He drew a distinction between the 16-hour detention at issue in *Montoya de Hernandez* and the limited inconveniences, such as questioning, patdowns, and searches of luggage, that occur in routine border search cases:

> These [routine] measures, which involve relatively limited invasions of privacy and which typically are conducted on all incoming travelers, do not violate the Fourth Amendment given the

---

[39] *Id.* at 541.

[40] Terry v. Ohio, 392 U.S. 1 (1968).

[41] *Montoya de Hernandez*, 473 U.S. at 543.

[42] *Id.*

> interests of "national self protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."[43]

Justice Brennan distinguished the detention of the defendant. First, the purpose was for criminal investigation, not protection of the sovereign.[44] If the government was truly concerned about preventing the entry of drugs into the interior, customs could have done a more thorough job at securing the defendant's passage out of the country.[45] Second, a person's diminished expectation of privacy at the border is not nil. Justice Brennan wrote:

> I do not imagine that decent and law-abiding international travelers have yet reached the point where they "expect" to be thrown into locked rooms and ordered to excrete into wastebaskets, held incommunicado until they cooperate, or led away in handcuffs to the nearest hospital for exposure to various medical procedures—all on nothing more than the "reasonable" suspicions of low-ranking enforcement agents.[46]

He noted that extended and intrusive detentions have typically fallen within the traditional Fourth Amendment requirements of probable cause and a warrant.[47]

The "non-routine" border search cases, like *Montoya de Hernandez*, have involved searches of the "alimentary canal"—the digestive track of a person. On one occasion, however, the Supreme Court had the opportunity to decide to what extent, if any, a search of property can be considered "non-routine." In *United States v. Flores-Montano*,[48] the defendant was stopped as he drove into a fixed checkpoint at the United States-Mexico border. After a brief inspection,

---

[43] *Id.* at 551 (quoting *Carroll*, 267 U.S. at 154).

[44] *Id.* at 564.

[45] *Id.*

[46] *Id.* at 560.

[47] *Id.* at 552-58.

[48] 541 U.S. 149 (2004).

Customs agents decided to remove the car's gas tank because they suspected that it contained drugs. Indeed, after a mechanic detached the gas tank—a process that took 15 to 25 minutes—agents found 37 kilograms of marijuana bricks. On appeal, the government specifically conceded that the customs officials did not have reasonable suspicion to conduct the search, even though the facts of the case indicated that they did. A customs officer at the primary checkpoint had tapped on the gas tank and thought that it sounded "solid." The government elected not to argue that the officials had reasonable suspicion; it did so in order to challenge an earlier Ninth Circuit decision[49] that held that reasonable suspicion was required to remove a gas tank from a car at the border.

Writing for a unanimous Court, Chief Justice Rehnquist held that the removal of the gas tank was constitutional, notwithstanding the absence of any degree of suspicion. The Court declined to find that this was a "non-routine" border search. "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[50] "Time and again," the Court said, it had upheld searches at the border because the sovereign has a longstanding and "inherent" right to protect itself at the border.[51] The Court also noted the long history of both legislative and judicial approval for such searches. In rejecting the defendant's arguments that the search unreasonably violated his right to privacy, the Court recognized that the "expectation of privacy is less at the border than it is in the interior."[52] The Court found no evidence in the record that the temporary removal of the gas tank caused long-term damage to

---

[49] *See* United States v. Molina-Tarazon, 279 F.3d 709 (9th Cir. 2002).

[50] *Flores-Montano*, 541 U.S. at 152-53.

[51] *Id.*

[52] *Id.* at 154.

the vehicle. The Court left for another day whether a "different result" would be required if a search of property resulted in damage or was conducted in a particularly offensive manner.[53]

In the context of laptop searches, the question is this: Are they "routine: searches, which require no suspicion and may be done at random, or are they "non-routine," like the search and seizure in *Montoya de Hernandez*, which require, at a minimum, reasonable suspicion? The cases to have addressed this question have held that they fall under the former category.

In *United States v. Ickes*,[54] the Fourth Circuit affirmed a defendant's conviction for transporting child pornography. The defendant was stopped as he crossed the Canadian-U.S. border. A search of his van found a computer and 75 disks containing child pornography, including a video of the defendant fondling the genitals of two young children. The Fourth Circuit began its analysis by poignantly noting, "However the Constitution limits the government's ability to search a person's vehicle generally, our law is clear that searches at the border are a different matter altogether."[55] The court rejected the defendant's argument that the search was conducted in violation of 19 U.S.C. § 1581(a). This statute had historically been construed in an "expansive manner."[56] In rejecting the defendant's constitutional challenge, the Fourth Circuit applied the holding in *Ramsey* and found the search of the computer disks to have been lawful. It declined to carve out an exception for "expressive material."[57] "Particularly in today's world, national security interests may require uncovering terrorist communications,

---

[53] *Id.* at 155-56.

[54] 393 F.3d 501 (4th Cir. 2005).

[55] *Id.* at 503.

[56] *Id.* at 505.

[57] *Id.* at 506.

which are inherently 'expressive.'"[58] The court discounted the defendant's argument that, under the government's argument, any person on an international flight could have his or her laptop computer's hard drive exhaustively searched. The unanimous court found this idea "far-fetched" because Customs agents do not have the time or resources to search the contents of every computer that crosses the border.[59] "As a practical matter," the Court stated, "computer searches are most likely to occur where—as here—the traveler's conduct or the presence of other items in his possession suggest the need to search further."[60]

Two cases from the Ninth Circuit followed *Ickes* and directly involved laptop computers. In both cases—*United States v. Romm*[61] and *United States v. Arnold*[62]—the defendants were stopped at international airports after arriving from foreign countries and had their laptop computers searched. In both cases, Customs agents found child pornography on the laptops' hard drives and the Ninth Circuit upheld the searches as constitutional. In *Romm*, however, the court declined to address the defendant's argument that the search of the laptop was "too intrusive" to qualify as a "routine" border search because he had raised this issue for the first time in his reply brief to the appellate court.[63] (Likewise, in *United States v. Irving*,[64] the Second Circuit rejected a challenge to the search of floppy disks at the border, finding that the search

---

[59] *Id.* at 507.

[60] *Id.*

[61] 455 F.3d 990 (9th Cir. 2006).

[62] 523 F.3d 941 (9th Cir. 2008).

[63] *Romm*, 455 F.3d at 997.

[64] 432 F.3d 401 (2d Cir. 2005).

was based on reasonable suspicion. Therefore, that court did not have the opportunity to address whether the search was routine or non-routine.)

In *Arnold*, however, the Ninth Circuit squarely addressed whether the search of a laptop at the border is routine or non-routine. In reversing the district court's order suppressing the fruits of the search, the Ninth Circuit concluded that the search was routine and the government was not required to establish that its agents had reasonable suspicion. The court rejected the district court's use of a "sliding intrusiveness scale to determine when reasonable suspicion is needed to search property at the border"[65] because of the Supreme Court's disapproval, in *Flores-Montano*, of "[c]omplex balancing tests" to determine what is a routine search.[66] The defendant attempted to distinguish this portion of *Flores-Montano* by noting that it was in the context of vehicle searches. The Ninth Circuit, however, recognized that, "The Supreme Court's analysis determining what protection to give a vehicle was not based on the unique characteristics of vehicles with respect to other property, but was based on the fact that a vehicle, as a piece of property, simply does not implicate the same 'dignity and privacy' concerns as 'highly intrusive searches of the person.'"[67] Finally, the court found that neither of the two possible exceptions left open by *Flores-Montano* was applicable. The defendant's laptop was not damaged and there was nothing to indicate that Customs searched the laptop in a "particularly

[65] *Arnold*, 523 F.3d at 945.

[66] *Id.* at 946.

[67] *Id.* (*quoting Flores-Montano*, 541 U.S. at 152).

offensive manner."[68] A petition for rehearing *en banc* is presently pending before the Ninth Circuit.[69]

III. Resolution of the Competing Policy Interests

I submit that the laptop border search cases have correctly applied the law. *Ramsey* established a necessarily broad rule for searches at the international border. The nation has an inherent right to protect itself and to interdict the importation of harmful items. The ability to conduct suspicionless searches is a vital tool to prevent narcotics, weapons, drug money, untaxed imports, child pornography, and disease-carrying plants and animals from entering the country. At the same time, persons have a diminished expectation of privacy at the border. Travelers in the modern age—particularly those who travel internationally—know and expect that they will be subject to search without cause at multiple points in their journeys.

The courts have correctly rejected attempts to analogize laptop searches to the type of search and seizure conducted in *Montoya de Hernandez*. Defendants have argued that the situations are similar because of the highly private information contained on some laptop computers. This argument is unavailing. The search and seizure in *Montoya de Hernandez* was considered "non-routine" not just because it was an intrusion into the defendant's privacy. The Court's decision was also based on the fact that there was a unique "interest[] in human dignity" that was at stake.[70] A laptop computer—no matter the quantity or nature of the information

---

[68] *Id.* at 946-47.

[69] *Arnold* was cited favorably in a recent district court decision. *See* United States v. Bunty, 2008 WL 2371211 (E.D. Pa. June 10, 2008) (Kauffman, J.) ("Although the Supreme Court has not addressed specifically the search of computer equipment at the border, other federal courts have agreed that such searches do not require reasonable suspicion.").

[70] *Montoya de Hernandez*, 473 U.S. at 540 n.3.

contained within it—simply does not implicate the same degree of privacy concerns involved with a person's "alimentary canal."

Nevertheless, the Constitution, and the courts' interpretation of its text, only sets a minimum standard for civil rights and liberties. Of course, Congress and the Executive have the authority to set laws and policies that exceed these constitutional protections, if doing so would provide greater protection for privacy and individual rights. It is this broader question that I will now address. The appropriate inquiry, in the context of policy-making, should involve a careful balancing of the competing interests at stake: the government's interests in conducting suspicionless searches versus the privacy interests of those crossing the border.

Opponents[71] of border searches of laptops point to the personal and private information, such as Internet browsing history, e-mails, and financial records, that are contained on some laptops. There is a correspondingly high expectation of privacy, they argue, that warrants a requirement of reasonable suspicion.

There is no doubt that many people keep personal information on their laptop computers. But the same can be said for the traveler who keeps his checkbook, notes for an upcoming novel, medications, photographs, sketches for a new invention, political literature, love letters, and personal diary in his briefcase. No one doubts that each of these items can be seen and examined by Customs officials at the border without a requirement of reasonable suspicion.

So the question becomes whether a laptop is, by its very nature, sufficiently different that it warrants a categorical exception to the general rule. Stated another way, should the "high-

---

[71] *See, e.g., Brief for Amici Curiae Association of Corporate Travel Executives and Electronic Frontier Foundation in Support of Appellee's Petition for Rehearing En Banc*, United States v. Michael Timothy Arnold, No. 06-50581 (9th Cir.); Jeanne Meserve, *Suit: Airport searches of laptops, other devices intrusive*, http://www.cnn.com/2008/TRAVEL/02/11/laptop.searches/index.html (accessed June 21, 2008).

tech" traveler receive special treatment because he carries his private information electronically, rather than in a more traditional form? Certainly more information can be kept on a computer than can be stored in a briefcase. The international traveler, however, can control how much of this information can be seen by the government. Files that are not necessary for a specific trip can be kept at home or at one's business. Opponents would likely counter that even "deleted" files can be retrieved by government technicians. This is true. However, this argument assumes that the government has the time and manpower to do so in every case. As a practical matter, the government would more likely reserve those resources for cases in which its agents already had some suspicion that the laptops contained something illegal, as the Fourth Circuit recognized in *Ickes*.[72]

In addition, there is an even less of a reasonable expectation of privacy at the international border because of the nature of international travel. Countries, including the United States, randomly search travelers at both entry and exit.[73] So a person who travels from, say, China to the United States, will be subject to, at a minimum, two searches: upon exiting China and upon entering the United States. Likewise, a person who travels in the opposite direction will face a search upon departure from the United States, by American authorities, and again before being permitted to enter China, by Chinese customs officers. I submit that many countries conduct much more aggressive searches than the United States. The international traveler should expect, then, that he will encounter several searches of his person or property and that some will

---

[72] "As a practical matter, computer searches are most likely to occur where—as here—the traveler's conduct or the presence of other items in his possession suggest the need to search further."

[73] Exit searches were the subject of my law review article, *The Border Search Exception for Exports: A Global Conceptualization*, 26 Quinnipiac L. Rev. 1 (2007). Exit searches are justified for myriad reasons, including the need to ensure that appropriate duties and taxes have been paid, that travelers are not smuggling high technology, and that unreported currency, which is the lifeblood of the international drug trade, is not leaving the country.

be more invasive than others. Therefore, even if the United States adopted a rule requiring reasonable suspicion for searches of laptops, international travelers would still face a diminished expectation of privacy because their computers could still be randomly searched by the foreign country that they were visiting or leaving.

All of these privacy considerations must then be balanced against the government's legitimate interests in conducting suspicionless searches of laptops and other electronic devices. The reported cases on this subject involved individuals attempting to bring child pornography into the country. Congress itself has recognized the dangers associated with such imagery by providing for steep penalties for its importation, distribution, and possession. Additionally, there is the potentiality for terrorists and international criminal organizations to use laptops as a means of secreting files, plans, and messages into the country for distribution to cells and allies within the interior of the country. Presently, the threat of random, suspicionless searches may be deterring such means of communication. Given the possibility of surveillance of phones and the Internet, "old fashioned" smuggling across the border, by storing files on a laptop, might prove a safer and more attractive alternative for such communication provided the persons doing so could be assured that the computer would not be subject to the possibility of random and suspicionless search.

There is an additional problem with creating a special exception for laptops at the border: defining its scope. Should reasonable suspicion be required for searches of flash drives and other storage media? What about Blackberry and other PDA devices? Why not extend protection to equally private containers of information, such as the films and videos that were at issue in the early civil forfeiture cases? This highlights the problem of deviating from a categorical rule in

this area. We have a privacy interest in nearly everything we own or bring across the border—no person wants the government "snooping" through his laptop any more than his briefcase, checkbook, medications, clothing, books, Blackberry, or digital media. It would be difficult to avoid having the exception swallow the rule.

I have confined my analysis to the question of laptop *searches*. Seizures of such devices are another matter altogether. The border exception justifies the search, not the seizure, of items that cross the border. In order to seize an item, the government must have probable cause that the item is, or contains, contraband. If a Customs officer finds child pornography on a laptop, for example, he or she would be justified in seizing the computer since it contains contraband and persons do not have a right to retain contraband. I am aware of no authority that would permit the government, without probable cause to believe it contains contraband, to keep a person's laptop or to copy the contents of its files.

IV. Some Modest Proposals

During oral argument in *Flores-Montano*, it came to light that Customs keeps a record of all border searches that its agents conduct and the reasons, if any, for each particular search.[74] If this is the still the case, the records should provide Congress with enough information to determine whether laptop searches are being conducted in a abusive or racially discriminatory manner.[75] Given the highly sensitive nature of such records, such review should be kept under seal, in the same manner that, for example, information about the number of air marshals is kept

---

[74] *Flores-Montano*, 541 U.S. at 156 (Breyer, J., concurring).

[75] *Id.* ("This administrative process should help minimize concerns that gas tank searches might be undertaken in an abusive manner.").

out of the public record.[76] If such records are no longer being kept, it might be advisable for the practice to be restarted.

The Executive Branch can take administrative and rule-making steps, in addition to record-keeping, to ensure that privacy intrusions are kept to a minimum. For example, at the traveler's request, an examination of a computer should occur away from public view. Only officers who have received appropriate training should be allowed to conduct searches, in order to minimize the possibility of irreparable damage to, or erasure of, files and the hardware itself. A rule requiring searches to be conducted in the presence of a supervisor would also be prudent.

Conclusion

Any search at the border will be viewed, by the person being searched, as a "violation of privacy." The Constitution recognizes, however, that such "violations" are nevertheless permissible if they are "reasonable" in the broader context of the legitimate government interests at stake. The government's interest in protecting the nation is at its zenith at the international border. At the same time, a person's *legitimate* expectation of privacy is at its lowest. To create a special exception for laptop computers at the border would set a curious precedent, since there are innumerable other types of property in which a similarly strong argument about privacy could be made. At the same time, such an exception would open a vulnerability in our border by providing criminals and terrorists with a means to smuggle child pornography or other dangerous and illegal computer files into the country.

---

[76] *See* http://www.tsa.dhs.gov/approach/mythbusters/fams_shortage.shtm.

I thank the subcommittee again for the invitation to testify here today. I would be glad to answer any questions. I can be reached via phone at (212) 920-4623 or via e-mail at larry.cunningham@yahoo.com.

Opening Statement of U.S. Senator Feingold
At the Senate Judiciary Committee
Subcommittee on the Constitution Hearing on
"Laptop Searches and Other Violations of Privacy Faced by Americans
Returning from Overseas Travel"
June 25, 2008

Good morning, and welcome to this hearing of the Constitution Subcommittee entitled "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel." We'll be hearing this morning from a panel of experts who can help us explore the legal and practical implications of this important issue.

If you asked most Americans whether the government has the right to look through their luggage for contraband when they are returning from an overseas trip, they would tell you yes, the government has that right. But if you asked them whether the government has a right to open their laptops, read their documents and e-mails, look at their photographs, and examine the websites they have visited, all without any suspicion of wrongdoing, I think those same Americans would say that the government absolutely has no right to do that. And if you asked them whether that actually happens, they would say, "not in the United States of America."

But it is happening. Over the last two years, reports have surfaced that customs agents have been asking U.S. citizens to turn over their cell phones or give them the passwords to their laptops. The travelers have been given a choice between complying with the request or being kept out of their own country. They have been forced to wait for hours while customs agents reviewed and sometimes copied the contents of the electronic devices. In some cases, the laptops or cell phones were confiscated, and returned weeks or even months later, with no explanation.

Now, the government has an undeniable right and responsibility to protect the security of our borders. The Supreme Court has thus held that no warrant and no suspicion is necessary to conduct, quote, "routine searches" at the border. But there is a limit to this so-called "border search exception." The courts have unanimously held that invasive searches of the person, such as strip searches or x-rays, are "non-routine" and require reasonable suspicion. As the Supreme Court has stated, these searches implicate "dignity and privacy interests" that are not present in routine searches of objects.

So the constitutional question we face today is this: When the government looks through the contents of your laptop, is that just like looking through the contents of a suitcase, car trunk, or purse? Or does it raise dignity and privacy interests that are more akin to an invasive search of the person, such that some individualized suspicion should be required before the search is conducted?

This administration has argued in court that a laptop can be searched without any suspicion because is no different from any other, quote, "closed container." I find that argument disingenuous, to say the least. The search of a suitcase – even one that contains a few letters or documents – is not the same as the search of a laptop containing files upon files of photographs, medical records, financial records, e-mails, letters, journals, and an electronic record of all websites visited. The invasion of privacy represented by a search of a laptop differs by an order of magnitude from that of a suitcase.

Ultimately, though, the question is not how the courts decide to apply the Fourth Amendment in these uncharted waters. I guarantee you this: neither the drafters of the Fourth Amendment, nor the Supreme Court when it crafted the "border search exception," ever dreamed that tens of thousands of Americans would cross the border every day, carrying with them the equivalent of a full library of their most personal information. Ideally, Fourth Amendment jurisprudence would evolve to protect Americans' privacy in this once unfathomable situation. But if the courts can't offer that protection, then that responsibility falls to Congress. Customs agents must have the ability to conduct even highly intrusive searches when there is reason to suspect criminal or terrorist activity, but suspicionless searches of Americans' laptops and similar devices go too far. Congress should not allow this gross violation of privacy.

Aside from the privacy violation, there is reason for serious concern that these invasive searches are being targeted at Muslim Americans and Americans of Arab or South Asian descent. Many travelers from these backgrounds who have been subject to electronic searches have also been asked about their religious and political views. As we'll hear today, travelers have been asked why they chose to convert to Islam, what they think about Jews, and their views of the candidates in the upcoming election. This questioning is deeply disturbing in its own right. It also strongly suggests that border searches are being based at least in part on impermissible factors.

The disproportionate targeting of this group of Americans does not mean that other Americans are exempt. The Association of Corporate Travel Executives has surveyed its members, and seven percent of business travelers who responded to the survey had experienced seizures of their laptops or other electronic equipment. That's an incredible number, when you consider how many Americans are

required to undertake overseas business travel today and the amount of confidential business information stored on their laptops. As we'll be hearing today, the problem is large enough to have a real impact on the way Americans do business.

Americans have tried to find out from DHS what its specific policies are on searching and seizing electronic equipment at the border. Two non-profit organizations filed a Freedom of Information Act request in October 2007 to get DHS to turn over its policies. Eight months later, DHS has not complied with that request. My own questions for Secretary of Homeland Security Michael Chertoff on this issue, which I submitted to him in early April after his appearance at an oversight hearing held by the full Judiciary Committee, have not been answered, despite my specific request that they be answered before this hearing.

I asked DHS to send a witness to testify today. DHS responded that its preferred witness was unavailable on the day of the hearing. I asked DHS to send a different witness, but DHS declined. I felt it was so important to have a DHS witness here that I wrote a letter to Secretary Chertoff last week urging him to reconsider. That letter will be made part of the hearing record. I would put the Secretary's response in the record, as well, but he has not responded.

DHS did provide written testimony. That testimony, which incidentally was submitted over 30 hours later than the committee's rules require, provides little meaningful detail on the agency's policies and raises more questions than it answers – questions that no one from DHS is here to address.

Needless to say, I'm extremely disappointed that DHS would not make a witness available to answer questions today. Once again, this administration has demonstrated its perverse belief that it is entitled to keep anything and everything secret from the public it serves and their elected representatives, while Americans are not allowed to keep any secrets from their government. That's exactly backwards. In a country founded on principles of liberty and democracy, the personal information of law-abiding Americans is none of the government's business, but the policies of the government are very much the business of Congress and the American people.

In any event, I look forward to hearing from the witnesses who did accept my invitation to testify today, so we can begin to explore this important issue in more detail.

RUSSELL D. FEINGOLD
WISCONSIN

506 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5323
(202) 224-1280 (TDD)
feingold.senate.gov

United States Senate

WASHINGTON, DC 20510-4904

COMMITTEE ON THE BUDGET
COMMITTEE ON FOREIGN RELATIONS
COMMITTEE ON THE JUDICIARY
SELECT COMMITTEE ON INTELLIGENCE
DEMOCRATIC POLICY COMMITTEE

June 19, 2008

The Honorable Michael Chertoff
Secretary of Homeland Security
Department of Homeland Security
Washington, DC 20528

Dear Secretary Chertoff:

On June 11, my office contacted the Department of Homeland Security's Office of Legislative Affairs to request that DHS provide a witness to testify at the June 25 hearing of the Senate Judiciary Committee's Constitution Subcommittee entitled "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel." Yesterday, DHS informed my office that the Department is declining to send a witness to testify. I am writing to urge you to reconsider this decision and to make a witness available who can testify about DHS policies and practices with regard to searching the contents of laptops and other digital devices belonging to U.S. citizens.

The issue of suspicionless border searches of the contents of laptops and other digital devices is of great importance to the traveling American public, as well as to the American business community. One of the primary concerns is the lack of information about DHS policies regarding the search and seizure of digital information. In October 2007, two non-profit organizations filed a request under the Freedom of Information Act in order to obtain this information, but DHS has still not disclosed its policies in response to that request. Following the April 2 Judiciary Committee hearing on DHS Oversight, I sent you several questions in an effort to learn what DHS border search policies are; I have yet not received any response to those questions. Given DHS's non-responsiveness when members of the public and Congress have sought information on this issue, it is all the more important to have a witness present at the upcoming hearing to explain DHS policies and practice.

I understand that DHS initially indicated that Deputy Commissioner of Customs and Border Patrol Jayson Ahern was the appropriate person to testify, but that he would not be available on June 25. DHS asked that the hearing be postponed. Certainly, if it were reasonably possibly to accommodate such a request, I would do so. At this point, however, the Committee schedule and the schedules of other witnesses, particularly those who had already made arrangements to travel from out of state, prevent me from rescheduling the hearing. When my office informed DHS that rescheduling was not possible on this occasion, DHS responded that the agency would decline to send a witness.

○ 1600 ASPEN COMMONS
ROOM 100
MIDDLETON, WI 53562
(608) 828-1200
(608) 828-1215 (TDD)

○ 517 EAST WISCONSIN AVENUE
ROOM 408
MILWAUKEE, WI 53202
(414) 276-7282

○ 401 5TH STREET
ROOM 410
WAUSAU, WI 54403
(715) 848-5660

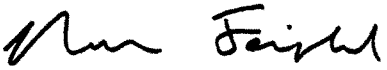
○ 425 STATE STREET
ROOM 225
LA CROSSE, WI 54601
(608) 782-5585

○ 1640 MAIN STREET
GREEN BAY, WI 54302
(920) 465-7508

I am very disappointed by this response. The purpose of inviting a DHS witness was not to get the perspective of a particular official, but to allow the agency to identify and explain its policies and be questioned about them. While I appreciate that Mr. Ahern may be the person with the most detailed knowledge of the issue in question, he is certainly not the only person within DHS who is familiar with Customs border search policies. The hearing was noticed two weeks in advance and DHS was given notice of the hearing on that same day. This should have been sufficient time for another DHS official or employee to consult with Mr. Ahern or undertake whatever additional preparation might be necessary.

The American people need and deserve answers about the policies that govern DHS searches of laptops, cell phones, and other digital devices. Their ability to get those answers should not depend on the availability of a single career official at DHS. I respectfully request that you reconsider the decision not to send a witness to the June 25 hearing. I further request, regardless of whether a witness will attend, that you respond to the written questions that I submitted after the April 2 hearing and that DHS provide written testimony by 9:30 am on Monday, June 23, as required by the Committee's rules. I intend to proceed with this hearing, and I believe it is in the best interest of DHS and the country for full information on the Department's policies to be available at that time.

Sincerely,



Russell D. Feingold
United States Senator

RUSSELL D. FEINGOLD
WISCONSIN

506 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5323
(202) 224-1280 (TDD)
feingold.senate.gov

United States Senate
WASHINGTON, DC 20510-4904

COMMITTEE ON THE BUDGET
COMMITTEE ON FOREIGN RELATIONS
COMMITTEE ON THE JUDICIARY
SELECT COMMITTEE ON INTELLIGENCE
DEMOCRATIC POLICY COMMITTEE

August 13, 2008

The Honorable Michael Chertoff
Secretary of Homeland Security
Department of Homeland Security
Washington, DC 20528

Dear Secretary Chertoff:

In an interview that was posted on Wired.com, you were asked about DHS's policy on searching the contents of Americans' laptop computers when they return from overseas travel. You noted that DHS had recently posted its laptop search policy on the agency's website. The interviewer then recorded the following exchange:

> **Wired.com:** Wouldn't it allay the suspicions of the business community if you had a policy that says we only search through laptops if we have a good reason to do so?
>
> **Chertoff:** That's exactly what I put it up on the internet. It is on the web to say, 'We only do it when we put you into secondary and we only put you into secondary when there is a suspicion, when there is reason to suspect something.'

The policy that is posted on the Customs and Border Patrol website is markedly different from what you described. The posted policy, dated July 16, 2008, does not even mention secondary screening, let alone limit laptop searches to cases in which secondary screening is performed. More important, the posted policy expressly states that laptop searches may take place "absent individualized suspicion," which directly contradicts your statement that the policy only allows laptop searches "when there is reason to suspect something."

Even if the posted policy did limit laptop searches to the context of secondary screenings, your statement that "we only put you into secondary when there is a suspicion, when there is reason to suspect something" is inconsistent with the written testimony submitted by Deputy Commissioner of U.S. Customs and Border Protection Jayson Ahern for the June 25, 2008, hearing I held on this subject. Mr. Ahern stated that U.S. citizens at the border may be subject to a second level of inspection if there is some basis for suspicion or "if they have been selected for random compliance examination." Random selection is the very opposite of individualized suspicion.

I am working on legislation to govern the searches of laptop contents at the border. It is difficult to craft appropriately targeted legislation, however, when your public statements about DHS's current policy differ so dramatically from the publicly posted policy. Moreover, the public has a right to know whether DHS permits searches "absent

○ 1600 ASPEN COMMONS
ROOM 100
MIDDLETON, WI 53562
(608) 828-1200
(608) 828-1215 (TDD)

○ 517 EAST WISCONSIN AVENUE
ROOM 408
MILWAUKEE, WI 53202
(414) 276-7282

○ 401 5TH STREET
ROOM 410
WAUSAU, WI 54403
(715) 848-5660

○ 425 STATE STREET
ROOM 225
LA CROSSE, WI 54601
(608) 782-5585

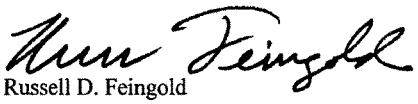
○ 1640 MAIN STREET
GREEN BAY, WI 54302
(920) 465-7508

individualized suspicion," as the posted policy states, or whether DHS only searches laptops in secondary screenings occasioned by individualized suspicion, as you stated in your Wired.com interview.

I therefore request that you inform me whether you intend to revise the posted policy to conform to your description of it or whether you will submit a correction to Wired.com, acknowledging that your statements about the posted policy were incorrect and that this policy does not limit laptop searches to secondary screenings occasioned by individualized suspicion.

I would appreciate a response to this letter within the next 10 days.

Sincerely,



Russell D. Feingold
United States Senator

JUN 25 2008

Office of Legislative Affairs
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

The Honorable Russell D. Feingold
United States Senate
Washington, DC 20515

Dear Senator Feingold:

On behalf of Secretary Chertoff, thank you for your letter of June 19, 2008, regarding the June 25, 2008, Senate Judiciary Committee's hearing entitled, "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel."

The Department of Homeland Security's (DHS) U.S. Customs and Border Protection (CBP) fully intends to comply with your request to provide written testimony to the Committee explaining CBP's position on searches regarding laptops and other electronic devices. DHS regrets that Deputy Commissioner Jayson Ahern is unable to attend the hearing in person due to his prior commitment to participate in the World Customs Organization meetings. Deputy Commissioner Ahern's written testimony relates to the questions the Committee posed on May 2, 2008. DHS's written response to your questions, pursuant to the April 2 hearing, is forthcoming.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

SEP 10 2008

Assistant Secretary for Legislative Affairs
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

The Honorable Russell D. Feingold
United States Senate
Washington DC 20510

Dear Senator Feingold:

On behalf of Secretary Chertoff, thank you for your letter of August 13, 2008, regarding inspection of electronic devices at U.S. ports of entry by U.S. Customs and Border Protection (CBP). You inquired whether Secretary Chertoff's comments to *Wired.com* were inconsistent with CBP's policy on border searches of information; in particular, his statement that searches occur only during secondary inspection and when "there is reason to suspect something." As explained below, the Secretary's statement is consistent with CBP's policy.

Under longstanding border search jurisprudence, the courts, including the Supreme Court, have recognized that the United States' constitutional authority to inspect – absent individualized suspicion – applies to information CBP may require to conduct its mission at the border. This authority has always covered information in containers, such as suitcases, briefcases, or laptop computers. This is necessary because, in addition to its border security mission, CBP is responsible for enforcing various copyright, export, import, and licensing laws, as well as criminal statutes pertaining to illegal information (such as child pornography). Requiring officers to specify individualized suspicions would drastically limit their ability to gather traveler's information effectively.

Container searches are performed only during secondary inspection due to the logistical limitations present at primary screening areas at most ports of entry. Travelers are referred for secondary inspection only when some level of suspicion exists. CBP's policy, which refers to absence of individualized suspicion, does not alter this ordinary practice. Once a traveler has been referred for secondary inspection, there is no additional burden the officer must meet to conduct a further inspection of that traveler's electronic devices.

Last year, nearly four hundred million travelers went through primary inspection at U.S. ports of entry. Less than two percent of those travelers were referred for secondary inspection. Of those, only a fraction had a laptop inspected by CBP. From August 1, 2008, to August 13, 2008, about 17 million travelers were encountered at ports of entry. Approximately 300,000 were referred for secondary inspection. Of those, a total of 40 were subject to a laptop inspection. This represents approximately 0.01 percent of all persons sent to secondary during that period and about 0.00025 percent of the total encountered at ports of entry.

CBP's longstanding border search policy results in a minimal burden on travelers. Codifying this policy or taking other steps that would limit or curtail the exercise of CBP's authority at the border could drastically impact CBP's ability to effectively discharge its mission of preventing dangerous people and materials from entering the country.

You noted that CBP Deputy Commissioner Jay Ahern testified at the July 25, 2008, hearing that persons may be subject to secondary inspection "if they have been selected for random compliance examination." Mr. Ahern was referring to an auditing program known as the Customs Compliance Measurement Examination (COMPEX). COMPEX – which is not mentioned in the CBP border search policy – is a longstanding program designed to allow CBP to develop a baseline from which it can measure how effective its officers are in detecting violations of law. Under COMPEX, of the four hundred million travelers encountered at ports of entry per year, approximately 0.065 percent are randomly referred to secondary inspection. In the event a traveler selected through COMPEX is carrying information in a container, such as a laptop computer, it is within the examining officer's discretion to decide whether and to what extent further inspection is needed.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Testimony of

Susan K. Gurley

Association of Corporate Travel Executives

Hearing on

Laptop Searches and Other Violations of Privacy

Faced by Americans Returning from Overseas Travel

United States Senate Committee on the Judiciary

Subcommittee on the Constitution

June 25, 2008

Chairman Feingold and distinguished members of this committee: I appreciate this opportunity to present the views of the Association of Corporate Travel Executives (ACTE) regarding the unrestricted authority claimed by the U.S. Department of Homeland Security (DHS) (including the U.S. Customs and Border Protection (CPB) and the Bureau of Immigration and Customs Enforcement (ICE)) to inspect, copy, or seize electronic devices – without provocation and/or suspicion – from any individual crossing a U.S. border. The seizure of laptops and other electronic devices is real and is not mere speculation.

ACTE at www.acte.org is the leading non-profit trade association providing education to the corporate travel industry. ACTE represents the safety, security, and service interests of all business travelers, and the financial concerns of more than 2,500 members from 82 countries, including the United States. ACTE's members represent an aggregate of $300

billion (USD) in annual business travel expenditures and include companies listed in the Fortune 1000 and Global 500. Business travelers contribute 65 percent of all airline revenue and represent the core customers of the hospitality industry in every major U.S. city.

ACTE's member companies have hundreds of thousands of travelers in the air at any given time. They routinely cross U.S. borders. ACTE represents billions of dollars in travel-generated taxes and many times that amount in direct expenditures, which support U.S. and global commerce. Even by a conservative estimate, this trickle-down effect of ACTE members on the overall American economic infrastructure is substantial. Moreover, it cannot be measured in dollars alone, but in jobs, innovation, corporate growth potential, company reinvestment, and ultimately stock value. The business traveler is a critical part of the U.S. – and the world's – economic future. The successful, seamless flow of business travel is critical to the American business profile and its influence in the global marketplace.

All international and U.S. business travelers who cross U.S. borders have two things in common: all carry electronic devices such as laptops, cell phones, Blackberries, iPods, and flash drives; and all are currently subject to the claimed authority of CBP or ICE officials to inspect and seize these electronic devices without provocation, suspicion, or warrant.

You will hear a number of compelling arguments today that these electronic devices are an extension of an individual's personal expression. You may also hear how the lack of established, published inspection procedures may lead to "profiling." Both of these are valid points. I am here to advise you that the unjustified retention and/or copying of proprietary and sensitive business information pursuant to the warrantless seizure of laptops and other electronic devices imposes both a personal and economic hardship on business travelers and their corporations.

In today's wired, networked and borderless world, one's office no longer sits within four walls or a cubicle; rather; one's office consists of a collection of mobile electronic devices such as

a laptop, a Blackberry/PDA, and a cell phone. It is common for business travelers to carry laptops and other electronic devices that contain both personal information (including health and financial records, addresses, etc.) and confidential business-related information (e.g. business plans, internal memoranda, contracts, passwords, and data). These devices constitute the office of today.

Under the U.S. Constitution, a warrant is needed to search a physical space, such as an office. Yet, the warrantless and unanticipated seizure of one's mobile office has been allowed to occur and can immediately deprive an executive or company of the very data – and revenue – a business trip was intended to create. As a businessperson returning to the U.S., you may find yourself effectively locked out of your office indefinitely and thereby deprived of the resources required to sustain your livelihood. Other rights are at stake as well. For example, the confiscation and downloading of a lawyer's client-related information could potentially violate attorney-client privilege. Similarly, the copying of a journalist's notes and interviews can impact the confidentiality of his/her sources and have a chilling effect on sources' willingness to speak to journalists.

There have been cases where information or hardware has been seized indefinitely, representing at a minimum a loss of the cost of the equipment either to the company or to the traveler. In the case of an independent entrepreneur, a laptop seizure can represent the loss of his or her entire business.

It can be argued that the percentage of seized computers and data is small in comparison to the total number of travelers crossing the border. However, because of a lack of transparency, the actual number of laptop seizures and the concurrent data downloading and potential data breach is not known to the public. ACTE surveyed its members in February 2008 on this issue; of the 100 people who responded, 7 reported that they had been subject to the seizure of a laptop or other electronic device. The survey also revealed that eighty-

one percent of survey respondents were unaware that the information on laptops and other electronic devices could be mirrored and held.

Even though the total number of business travelers subject to these searches and seizures can only be estimated, what is certain is the severe economic and behavioral impact that can follow when a laptop is seized. Some of the financial loss comes as a professional stigma associated with the seizure of one's laptop. Fifty percent of the respondents to ACTE's February 2008 survey indicated that having a laptop seized could damage a traveler's professional standing within a company.

Another concern is the lack of published U.S. government policies and DHS regulations that inform the public as to the government security measures in place to protect data when it is downloaded, who will have access to this information, how long the information can be stored and where it is stored, and how it will eventually be disposed of. The Government Accountability Office does not give high marks to the U.S. Department of Homeland Security and/or the U.S. Transportation Security Administration for data protection. The seizure of data or computers carrying corporate sales strategies, business plans, pending patents, or other sensitive proprietary information, could force these companies to implement new and expensive internal travel policies to counter potential data leaks and/or seizure.

In fact, this is already happening. Measures that companies are taking include sending data to themselves via web-accessible email, encrypting files, or using secure USB drives. In addition, companies are purchasing additional computers that are scrubbed of any prior emails so that they can easily be replaced. Furthermore, it is our understanding that some senior executives are prohibited from carrying any computers. All of these measures and business behavior changes cost time and money.

The title of this hearing is: "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel." But the fact is that laptops are also being

seized without recourse from foreign businessmen, journalists, and others – who are not U.S. citizens – without justification. ACTE is here to represent their interests as well.

According to a March 2008 release from the Travel Industry Association, "the United States welcomed 9 million fewer overseas visitors in 2007 than it would have if it had simply kept pace with post-9/11 worldwide long-haul travel trends. This decline has a serious economic impact resulting in a loss of billions of dollars of new visitors spending." This decline includes fewer foreigners attending conferences, meetings, and conventions in the U.S. ACTE believes that part of this decrease is due to the perception that the U.S. has withdrawn its welcome mat and made it difficult for visitors to come to the U.S. The U.S. cannot afford to be viewed as unwelcoming and thereby lose an opportunity for a visitor to attend a meeting for the first time in the U.S. and have a positive U.S. experience. The concurrent worry that their laptop (or other electronic equipment) may be seized and their personal, financial, health, and/or business information downloaded, adds to the perception that the U.S. is no longer a welcoming country.

In the June 11, 2008 edition of USA Today, a front-page article discussed the fact that the U.S. government is warning U.S. visitors to the Beijing Olympics that their laptops are likely to be penetrated by the Chinese government aiming to steal trade and business related secrets. Yet the U.S. government effectively does the same thing by seizing computers or electronic data, without explanation, and without apparent safeguards. Does the U.S. want to be perceived in the same light as the Chinese government when it comes to downloading information from laptops?

ACTE urges Congress to clarify border procedures – especially those entailing laptop seizures and the inspection of proprietary and personal data. We understand and support reasonable measures to protect the integrity of the U.S. border and the safety of its people. However, we believe these objectives can be met without sacrificing due process of law.

This might entail legislation to require, at a minimum, "reasonable suspicion" to search or seize electronic devices and their electronic files.

Finally, we are requesting improved and transparent communications from DHS (including ICE and CBP) regarding the policies and safety measures that they have in place to protect downloaded data and/or seized laptops in cases where the legal standard for seizure is satisfied. We request that the Committee undertake the following:

- Request a privacy impact assessment from the CPB on the number of seizures of laptops or other electronic devices; the minimum, average, and maximum amount of time that it takes to return the laptop and or other electronic device to the owner; and the reasons for the seizures.
- Require that the policies regarding laptop seizures be published by DHS in the Federal Register and on the agency's home page under quick links (http://www.cbp.gov/xp/cgov/travel/). This would allow any traveler to go to the site and know his/her rights. These policies should include, at a minimum, the following:
    - Policies for protecting the integrity of the data;
    - Policies for the length of time seized data will be stored and where and how it will be stored;
    - Policies for whether the downloaded information will be shared and, if so, with what other U.S. government and international agency(s) and under what circumstances;
    - Policies for who within the federal government will have access to the information;

- Information as to what rights a traveler has to ensure that his/her laptop and/or other electronic devices are returned; and
- A requirement that a receipt be given immediately to anyone whose laptop is seized with information regarding whom to call for information about the seizure.

Ultimately, ACTE would like Congress to consider laptops and other electronic devices as an extension of an individual's personal and professional identity and uniquely different from other forms of baggage.

In conclusion, I would ask the members of this committee to consider the following analogy. The hearing today is taking place in a federal building. All visitors meeting with their Senators are subject to a possible search and some kind of inspection. Suppose that search was extended to include the contents of all cell phones, Blackberries, and other electronic devices. Suppose too that the electronic devices constituents brought with them were seized and copied. Would you allow the seizure of your constituents' property and data, perhaps indefinitely, without a warrant and/or justification? This is essentially what is happening to our constituents – who are also your constituents – at the U.S. borders.

The Association of Corporate Travel Executives would like to thank Chairman Feingold and this committee for responding to an issue that will have long-term implications for corporate America, the international traveling public, and the global economy. The resources of our association are at the disposal of this committee and DHS and its Border Protection authorities.

Testimony of

Farhana Y. Khera
President & Executive Director, Muslim Advocates

Hearing on
Laptop Searches and Other Violations of Privacy
Faced by Americans Returning from Overseas Travel

United States Senate Committee on the Judiciary
Subcommittee on the Constitution

June 25, 2008

Introduction

On behalf of Muslim Advocates, I welcome the opportunity to testify before the U.S. Senate Committee on the Judiciary, Subcommittee on the Constitution regarding invasive searches and interrogations at the nation's borders.

Muslim Advocates (www.muslimadvocates.org) is a national legal advocacy and educational organization dedicated to promoting and protecting freedom, justice and equality for all, regardless of faith, using the tools of legal advocacy, policy engagement and education and by serving as a legal resource to promote the full participation of Muslims in American civic life. Founded in 2005, Muslim Advocates is a sister entity to the National Association of Muslim Lawyers, a network of over 500 Muslim American legal professionals. Muslim Advocates seeks to protect the founding values of our nation and believes that America can be safe and secure without sacrificing constitutional rights and protections.

Since September 11, 2001, the Muslim American community has been subjected to heightened scrutiny by law enforcement authorities, including "voluntary" interviews conducted extensively in the community by the FBI; the NSEERS registration program targeting males from primarily Muslim and Arab nations to comply with special registration requirements with the INS (and later DHS); and concerns about targeting the Muslim American community for data-gathering about where they live, their socio-economic status, their interest in alternative forms of media, associations with ethnic organizations, where they worship, and other private information.

Muslim Advocates has received a number of complaints from U.S. citizens and legal residents in the Muslim, Arab and South Asian American communities who have experienced invasive questioning, searches and seizures at airports or land crossings upon their return to the U.S. after international travel. These activities include searches and seizures of laptops, cell phones, and digital cameras, as well as questioning about individuals' associations, or religious or political beliefs and activities. These incidents raise concerns about:

(1) invasive questioning;
(2) invasive searches and seizures, especially of data-carrying devices; and
(3) discriminatory policing at the border.

The U.S. Department of Homeland Security (DHS) and Customs and Border Patrol (CBP) have a critical responsibility to protect our nation's borders, including barring entry to those who would seek to do our nation harm. At the same time, DHS and CBP officials, who have been granted enormous law enforcement power by the American people, have an obligation to wield that power consistent with the rights and protections guaranteed by the Constitution to all Americans, regardless of religion, ethnicity or race.

My testimony presents a number of incidents from across the country that suggest that the First and Fourth Amendment rights of innocent Americans are being violated. The

circumstances of these incidents also suggest that racial, ethnic and/or religious profiling is taking place at the border. My testimony therefore concludes with recommendations for Congress to help protect the rights of law-abiding Americans returning home.

Interrogations and searches at the nation's borders are invasive and pervasive.

Muslim Advocates and other civil rights groups have received numerous complaints from travelers who, upon re-entry to the U.S., are subjected to invasive questions and/or searches. Innocent Muslim, Arab and South Asian Americans from all walks of life have had their electronic devices searched by CBP agents, or have been interrogated by CBP agents about their political views and activities, religious beliefs and practices, and associations with organizations, friends and relatives – all without any reasonable suspicion that the individuals were engaged in unlawful activity.

Most of the complaints received involve experiences from 2007 to the present, at air and land ports of entry across the U.S., including Seattle, San Francisco, Houston, Detroit, Boston, and Newark. Although these complaints are not the result of a comprehensive study or a systematic collection of incidents, there is reason to believe that these cases are indicative of a pattern of similar cases at the border.

The following is a summary of some of the complaints received:

1. A corporate vice president of a major high-tech company based in the Seattle, WA area has been subjected to interrogations on at least eight separate occasions since Spring 2007. A business and community leader, he previously testified before the U.S. House of Representatives on measures to strengthen the American information technology industry and received the Walter Cronkite Faith and Freedom Award from the Interfaith Alliance Foundation in 2003. Since early 2007, he has traveled for business and personal reasons to a number of different countries, including Japan, Canada, United Kingdom (and other parts of Europe), and Turkey. Upon his return, CBP agents have interrogated him about the names, birth dates and addresses of family members living abroad and in the U.S., the identities of business and personal contacts with whom he met during his travels, his religious practices (e.g., which mosque he attends), and his activities on behalf of a Muslim charitable organization in the Greater Seattle area he helped establish, as well as the organization's activities. (This charity, which has never been designated as a terrorist organization, has worked closely with other faith communities in the Pacific Northwest as part of multi-faith efforts, including collaborative community service projects such as building homes for the needy.) CBP officials have searched his cell phone, made copies of various documents on several occasions, and extensively searched his belongings, as well as those of family members who traveled with him. This U.S. citizen has filed complaints with DHS, as well as the FBI and his members of Congress, but he has yet to receive a meaningful reply. One CBP agent told him that to avoid such interrogations he would have to cease international travel.

2. An American Muslim of Pakistani descent, who is a graduate of Georgetown University Law Center and now practicing with a major law firm on the west coast, was interrogated by CBP agents at San Francisco International Airport after visiting relatives overseas in the Spring 2008. Upon confirming her citizenship status, she thoroughly answered initial questions about her travels and identity. Nevertheless, without any reason to believe that this U.S. citizen was carrying prohibited items or was otherwise engaged in unlawful activity, the CBP agent arbitrarily insisted on searching her luggage, seized her digital camera and reviewed the images — reflecting pictures from her travel with her family, as well as various photos taken in the United States prior to her travel. The agent interrogated her about the identities of the people in her travel photos, their location, and her relationships to them. Upon seeing a book in her bag about a presidential candidate, the CBP agent then posed questions about her political views of candidates in the 2008 presidential election.

3. A firefighter, 20-year former member of the National Guard, Gulf War veteran, and current member of the local Homeland Security Emergency Response Team in Toledo, OH has been questioned on numerous occasions since 2006 at the Detroit Ambassador Bridge while trying to visit family members in Ontario, Canada.[1] He was detained at times for up to four hours. CBP agents have searched his car and his cell phone and have asked about why he chose to convert to Islam. In one encounter, CBP officials confronted him with a letter to the editor he wrote in a local Toledo newspaper criticizing U.S. foreign policy. CBP agents asked what inspired him to write it and whether he personally knew anyone mentioned in the piece. On at least ten occasions, he has been asked about any foreign associates he or his wife, who is of Lebanese descent, may have and his financial transactions.

   This military veteran has persistently sought redress for this scrutiny, but has only been told by DHS that his "records have been modified." After receiving this response, he has been detained at the border three additional times, during the most recent of which he was handcuffed in front of his children as a CBP agent said, "look at what you have got yourself into." He has also been intimidated at the border by a CBP agent who emptied and reloaded a gun while interrogating him.

4. An American Muslim graduate student at Yale University is frequently subjected to scrutiny when returning from international travel. This U.S. citizen is currently pursuing a doctoral degree in Islamic studies, has been cited by press outlets including *The Houston Chronicle* and *The Washington Post* as an expert on mainstream Islam and the integration of Muslims in the U.S., and has been consulted as an expert by federal government agencies, including the National

---

[1] *See U.S. Citizens Question Terror Watch Lists, CBS News (December 8, 2007), available at* http://www.cbsnews.com/stories/2007/12/08/eveningnews/main3595024.shtml.
See also Ellen Nakashima, *Collecting of Details on Travelers Documents*, WASHINGTON POST (September 22, 2007).

Counterterrorism Center and the Department of State. The scrutiny appears to have begun in 2005 and continues to the present. CBP agents at Newark International Airport have interrogated him several times about the contents of his lectures, the places where he has lectured, and even the mosques in which he has prayed. In addition, CBP agents at Houston Intercontinental Airport also interrogated him in Spring 2005 about his views of particular religious doctrines. CBP agents at various locations have photocopied his lecture notes on several occasions, and agents at the Niagara Falls border crossing in late 2005 seized and recorded data from his cell phone before interrogating him about his relationships with individuals who appeared in it. He has asked authorities both informally and formally about the basis for the apparent suspicion he has received. Citing national security concerns, however, authorities have denied him any explanation or guidance about how to relieve it.

5. A Muslim American of South Asian descent who is an engineer in the information technology sector was detained for several hours, searched and interrogated at San Francisco International Airport in Summer 2007 after returning from an overseas business trip that included a visit with family members. CBP agents searched and seized his checkbook and asked questions about his donations to specific charitable and religious organizations and his associations with specific Muslim community leaders in the San Francisco Bay Area. The agent demonstrated familiarity with the Muslim organizations and their leaders — none of whom have been designated by the federal government as entities or individuals with whom Americans are prohibited from doing business. After seizing (and ultimately confiscating) the traveler's cell phone, the agent advised him that he "would be in big trouble" if a search of its contents revealed the names of particular leaders of charitable organizations to which he had donated. This traveler's cell phone was ultimately returned, in a broken and inoperable condition, five months after this incident – around the same time that he became a naturalized U.S. citizen.

6. A San Francisco Bay Area software engineer reported being questioned for almost 20 hours after three international trips, despite hearing a CBP agent explain to another agent that he was not an actual match to a watch list. This U.S. citizen was asked about his religion, whether he hated the U.S. government, whether he had visited mosques, and even told that he should "pray more." When he offered to give one agent his wife's phone number so the agent could verify his identity, he was asked, "Isn't it rude in Islamic culture to give a man a woman's phone number?" Customs agents inspected his company laptop computer, examined all the books in his luggage, recorded information on one book about the Quran, and interfered when he attempted to take notes about the screening. Despite sending complaint letters to multiple federal agencies, he has been unable to resolve his situation.[2]

[2] This individual was identified through the Asian Law Caucus, a San Francisco-based civil rights organization.

7. A California businessman has been detained, interrogated, and searched numerous times upon his return to the United States. He has been asked what he thinks of Iran's president, whether he supports terrorism, whether he met any terrorists during the Hajj pilgrimage to Saudi Arabia, and what he thinks about Jews and the state of Israel. This U.S. citizen's laptop computer was removed from his presence for over two hours, and he was told that officers were examining all the files, including letters from his wife and children.[3]

8. A software engineer in Northern California has been subjected to scrutiny beginning in January 2007 at San Francisco International Airport after returning from a religious pilgrimage to Saudi Arabia. His digital camera was searched and CBP agents made him identify other people accompanying him on the pilgrimage who appeared in the pictures. In June and July 2007, this U.S. citizen was scrutinized during consecutive weekend trips to Canada for a self-development workshop organized by a Muslim organization. On each occasion his cell phone was searched and was used to search another SIM card he had. The interrogations lasted up to two hours, and his attempt to return from Ottawa, Canada in June 2007 was impeded by a detention, interrogation and laptop and cell phone search that forced him to miss his flight.[4] CBP agents posed questions about the particular conference he attended, its host, and the host's religious views. CBP agents questioned him at length about whether he believed the founder of the conference has ties to terrorists, and whether the traveler himself could have encountered terrorists, or terrorist sympathizers, at mosques he attends.

   Citing concerns about CBP agents recording his family members' information, this traveler chose to suspend international travel and has resumed only after purchasing an extra cell phone and laptop with no stored data. After the most recent interrogation in Toronto, Canada in July 2007, a CBP agent affirmatively apologized for posing such invasive questions and suggested that he was required to do so.

9. An American Muslim has been detained, questioned and searched at Logan International Airport on several occasions from 2002 to the present upon returning home from pursuing graduate studies abroad. CBP agents have searched his laptop computer on at least two occasions and have taken his flash drives and CD's to a back room where he presumes that the information has been copied. After confirming his citizenship, he has been asked about his religious practices, beliefs, and even directly challenged about why he is a Muslim.

Invasive interrogations and searches offend several core constitutional rights.

CBP practices described herein burden substantive constitutional rights, including the Fourth Amendment guarantee against unreasonable searches and seizures and the First Amendment freedom to maintain political views, religious practice and personal

[3] This individual was identified through the Asian Law Caucus.
[4] See Ellen Nakashima, *Clarity Sought on Electronic Searches*, The Washington Post (February 7, 2008).

associations without inviting government scrutiny. The recent decision of the U.S. Court of Appeals for the Ninth Circuit in *U.S. v. Arnold,* 2008 U.S. App. LEXIS 8590 (9th Cir., Apr. 21, 2008), holding that CBP can conduct searches of laptops without reasonable suspicion, magnifies these concerns. That decision effectively grants CBP the authority to conduct searches of Americans returning home arbitrarily and without cause.

The privacy, security and liberty interests of law-abiding Americans are at stake. In the wake of the *Arnold* decision, a broad array of over 20 civil libertarian, civil rights, interfaith and community organizations from across the ideological spectrum recently called on Congress to conduct oversight of CBP's investigatory activities at the border and to consider legislation to protect the constitutional rights of Americans returning home from international travel.[5]

Invasive questioning at the border about individuals' political opinions, religious views, or individuals' houses of worship, pilgrimage or other religious practice significantly burdens First Amendment rights to religious freedom and free expression. Invasive questioning about individuals' participation in charitable organizations or conferences or relationships with family and friends also significantly burdens the First Amendment right of association. Similarly, intrusive searches of digital cameras, cellular phones and handwritten notes place at risk of potential scrutiny the various subjects of a traveler's photos, cell phone contacts, or even people merely referenced in a traveler's private personal diary.

The statute creating DHS charged the new agency with securing the borders and preventing the entry of terrorists and instruments of terrorism into the United States. In the incidents described above, however, CBP appears to be asking questions about First Amendment protected activities and expression that are unrelated to specific criminal activity or border security.[6] Instead, these questions, as well as the invasive searches and seizures of electronic data, seem to be part of a general data-gathering activity by CBP. If so, a general data-gathering activity raises significant privacy and civil liberties concerns, including why this data is being gathered, who is being targeted, what data is being gathered, and how the data is being stored, shared and used.

---

[5] *See* Letter from Muslim Advocates, et al. to U.S. House of Representatives, Committee on Homeland Security, et al. (June 20, 2008), *available at* http://www.muslimadvocates.org/more.php?id=43_0_1_0_M; Letter from ACLU, Electronic Frontier Foundation et al. to U.S. House of Representatives, Committee on Homeland Security Committee (May 1, 2008), *available at* http://www.eff.org/press/archives/2008/05/01/border-search-open-letter; *U.S. v. Arnold*, 2008 U.S. App. LEXIS 8590 (9th Cir., April 21, 2008).

[6] We note that, to the extent the questioning is taking place without a tie to specific criminal activity, the nature of the setting – secondary questioning at a port of entry when an American, probably tired from a long flight, is seeking to get home – is coercive and would not be permissible in other settings within the U.S. For example, an FBI agent cannot detain a citizen within the country in order to interrogate him or her about religious practices, political views, or participation in local houses of worship or charitable organizations.

CBP's conduct raises concerns about racial, ethnic and religious profiling and runs counter to equal protection guarantees.

The complaints received from Muslim, Arab and South Asian Americans suggest that racial, ethnic or religious profiling is taking place at the borders and airports.

With the CBP asserting a broad authority to engage in searches, seizures and questioning, it raises legitimate concerns about how this authority is being carried out and whether there is an unfair and disparate impact on certain racial, ethnic or religious communities.[7] If, especially after the *Arnold* decision, a CBP agent is not required to have particularized suspicion to search or question, then there is an even greater likelihood that bias or impermissible factors can influence a CBP agent.

Such conduct would be wrong and in violation of the equal protection rights guaranteed by the Constitution. The administration has taken steps to end race or ethnic based profiling by federal law enforcement agencies. In 2001 during his first address to Congress, President Bush pledged to end racial profiling.[8] The U.S. Department of Justice (DOJ) later issued guidance purporting to ban racial and ethnic profiling by federal law enforcement agencies.[9] That DOJ Guidance stated:

> "Racial profiling in law enforcement is not merely wrong, but also ineffective. Race-based assumptions in law enforcement perpetuate negative racial stereotypes that are harmful to our rich and diverse democracy, and materially impair our efforts to maintain a fair and just society."

The DOJ Guidance then set forth the following principles:

> "In making routine or spontaneous law enforcement decisions, such as ordinary traffic stops, Federal law enforcement officers may not use race or ethnicity to any degree, except that officers may rely on race and ethnicity in a specific suspect description. This prohibition applies even where the use of race or ethnicity might otherwise be helpful."

---

[7] The Association of Corporate Travel Executives, law firms, high tech companies and other businesses that conduct international travel have also reported that electronic devices have been searched and seized. It appears, however, that intrusive questioning on First Amendment protected activities have focused primarily on travelers who are Muslim or of Arab or South Asian descent.

[8] *See* President George W. Bush, *Memorandum for the Attorney General* (Feb. 27, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/02/20010228-1.html; The White House, *Record of Achievement: Fighting Crime* (noting that "Less than six weeks after taking office, President Bush called for an end to racial profiling in Federal law enforcement."), *available at* http://www.whitehouse.gov/infocus/achievement/chap16.html.

[9] *See* Dep't of Justice, *Justice Department Issues Policy Guidance to Ban Racial Profiling* (June 17, 2003), *available at* http://www.usdoj.gov/opa/pr/2003/June/03_crt_355.htm ("The racial profiling guidance bars federal law enforcement officials from engaging in racial profiling . . . has been adopted by the President as executive policy for federal law enforcement, and governs all federal law enforcement activities . . . ."); *see also* Exec. Order No. 12,333, §2.4 ("Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad.").

> "In conducting activities in connection with a specific investigation, Federal law enforcement officers may consider race and ethnicity only to the extent that there is trustworthy information, relevant to the locality or time frame, that links persons of a particular race or ethnicity to an identified criminal incident, scheme, or organization. This standard applies even where the use of race or ethnicity might otherwise be lawful."

The DOJ Guidance then set forth two exceptions – for national security and border integrity. In these contexts, the DOJ Guidance states that federal law enforcement officers may not consider race or ethnicity except to the extent permitted by the Constitution or federal law.

The Department of Homeland Security subsequently adopted the DOJ Guidance:

> "It is the policy of the Department of Homeland Security to prohibit the consideration of race or ethnicity in our daily law enforcement activities in all but the most exceptional instances, as defined in the DOJ Guidance. DHS personnel may use race or ethnicity only when a compelling governmental interest is present. Rather than relying on race or ethnicity, it is permissible and indeed advisable to consider an individual's connections to countries that are associated with significant terrorist activity."[10]

At a hearing before the Senate Judiciary Committee on April 2, 2008, responding to a question from Senator Feingold, Homeland Security Secretary Michael Chertoff denied that ethnic profiling is taking place and explained that CBP agents consider factors such as individualized behavior and travel patterns in determining whether a U.S. citizen's connections to high risk countries merit further questioning and search.

While we welcome Secretary Chertoff's rejection of racial and ethnic profiling, DHS guidance allows him to do so. In addition, his response leaves unresolved the questions of how "individualized behavior" is defined and what factors are used by CBP agents to determine whether reasonable suspicion exists. For example, does CBP consider a traveler's appearance (e.g., wearing a beard or headscarf (hijab)) or nature of travel (e.g., religious pilgrimage) the basis for subjecting the traveler to secondary search and/or questioning? Similarly, is the country from which someone has traveled a proxy for religion or ethnicity? If so, these factors would be either discriminatory on their face, or so imprecise as to lead to a disparate impact on travelers who are Muslim or of Arab or South Asian descent.

Furthermore, the DHS guidance and Chertoff's assertions do not address concerns about religious or national origin profiling, which, like racial and ethnic profiling, should have been addressed by DOJ and DHS. Indeed, the fact that a number of complainants have

---

[10] *See* U.S. Dep't of Homeland Security, *The Department of Homeland Security's Commitment to Race Neutrality in Law Enforcement Activities* (June 1, 2004), *available at* http://www.dhs.gov/xlibrary/assets/CRCL_MemoCommitmentRaceNeutrality_June04.pdf.

noted that they have been asked about their religious practice and views underscores the need for clear federal authority – and ideally a federal law – on this issue.

Moreover, if CBP is found to be wielding its authority broadly, targeting Americans based on their religion or ethnicity, then CBP is not only engaging in discriminatory conduct, but has too much discretion, and the result is a waste of resources. Training and more rigorous scrutiny and oversight of CBP would improve security.

Finally, we note that DHS has rebuffed prior public requests to disclose its actual practices. Despite informal requests, as well as formal requests under the Freedom of Information Act filed by the Electronic Frontier Foundation and the Asian Law Caucus, DHS has refused to disclose meaningful information about any potential policies and procedures for interrogations, searches or seizures at the border.

Recommendations

Muslim Advocates urges the Committee to examine CBP and DHS border search and interrogation practices, and to consider legislative action to protect law-abiding Americans from arbitrary and invasive interrogations and searches when returning home from abroad.

1) Muslim Advocates recommends that Congress consider legislation that incorporates the following elements:

- Clarifies that searching data and electronic devices goes beyond a routine border search and requires reasonable suspicion.
- Clarifies that seizing data and electronic devices requires probable cause.
- Clarifies that questions about an individual's political or religious views or activities or lawful associations with individuals or groups are impermissible.
- Clarifies that the country from which an individual travels cannot be a pretext for religious, national origin or ethnic based investigatory activities.
- Clarifies that race, ethnicity, national origin or religion should not be considered in deciding upon the scope and substance of investigatory or other law enforcement activity, except where race, ethnicity, national origin or religion, along with other factors, is part of a suspect's description based on specific, credible information linking that suspect to a criminal incident.
- Requires CBP to report to Congress its policies and procedures on searches and questioning, including the standards for determining whether someone is sent to secondary inspection and whether to search or seize data or electronic devices, and the training that CBP agents receive to engage in questioning and electronic data searches and seizures, including copies of training materials and guidance.

- Requires CBP agents to collect data on border searches and interrogations and report this information to the public and to Congress, allowing Congress to monitor whether CBP policies are having a disparate impact on individuals based on their race, ethnicity, national origin, or religion. The data collected should include the CBP's agent's basis for reasonable suspicion (or probable cause, if a seizure of data or electronic devices) in flagging the individual for secondary inspection; the race, religion, ethnicity and national origin of the individuals stopped; whether data was searched; whether data or property was seized; and what kind of law enforcement action was taken based on the data seized or questions asked.

2) Muslim Advocates urges Congress to request that the General Accountability Office (GAO) conduct a thorough investigation and review of CBP policies and procedures, as well as actual practices, for selecting individuals for secondary inspection.

3) Muslim Advocates urges Congress to pass the *End Racial Profiling Act* (S.2481/H.R. 4611) ("ERPA"). As discussed above, there is need for a clear prohibition of racial, ethnic, national origin and religious profiling by federal law enforcement. The current DOJ guidance, and its adoption by DHS, does not explicitly prohibit profiling based on religion or national origin and contains overly broad exceptions for border security. In addition, data collection to allow the relevant federal agencies, Congress and the public to understand the scope of the problem and to monitor improvements in the application of solutions is critically needed. ERPA would address these concerns.

Congress must ensure that innocent, law-abiding Americans are able to travel freely, visit friends and relatives abroad, and engage in commerce, without fear that federal law enforcement will use the inherently coercive context of a border crossing to engage in violations of their privacy and First Amendment protected beliefs and activities. Congress must ensure that CBP both protects our nation and respects our nation's constitutional rights and protections.

Statement of Senator Patrick Leahy, Chairman
Senate Judiciary Committee
Subcommittee on the Constitution
"Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel"
June 25, 2008

I am glad Senator Feingold has convened this important hearing to examine intrusive practices by the Department of Homeland Security at our Nation's ports of entry. These practices affect the privacy interests of American citizens.

Americans understand that it is the Federal Government's responsibility to ensure that anyone entering the United States complies with the law. There is no dispute about this basic principle. But Americans also want their government's policies to respect and preserve our civil liberties. The government should not base its policies on racial profiling, act capriciously or be unnecessarily intrusive.

I share the concerns of privacy advocates about reports of highly intrusive searches carried out against American citizens returning home from abroad. In some instances, these searches are carried out based upon no reasonable suspicion, and delve deeply into the personal information of American citizens. In other instances, citizens have felt that the country to which they traveled or their personal appearance was the basis for increased scrutiny. When DHS officials routinely read the email, handwritten notes, and computer files of law-abiding Americans as they reenter the country, Americans are right to question this practice. And when DHS officials question Americans about their religious or political beliefs, and demand details of whom they met and where they slept during travel abroad, Americans are right to raise questions.

Two Circuit Courts of Appeal have held that the Fourth Amendment does not require any reasonable suspicion to search and seize the contents of any electronic device, including a laptop computer, belonging to an American citizen returning to the United States from abroad. It may surprise many Americans that their basic constitutional rights do not exist at our ports of entry even to protect private information contained on a computer. It concerns me, and I believe that actions taken under the cover of these decisions have the potential to turn the Constitution on its head.

Despite the extraordinary authority such rulings have sustained for the Department of Homeland Security, the administration and the Department's use of this power must be held to a standard consistent with our constitutional values. Where there are no constitutional safeguards, the environment becomes ripe for abuses, including racial, religious, and ethnic profiling. And by many accounts from business travelers and others, these practices are occurring.

American citizens subjected to practices that the Constitution would forbid anywhere else in the country have the right to be aware of the official policy and the rationale underlying the practice. Advocates have raised many very relevant questions about these

practices: How are individuals singled out for additional scrutiny? Where does any information go that is copied from a citizen's computer or electronic device? How does the agency dispose of gathered information that does not violate any law? How does the agency ensure that sensitive or proprietary information is not released? In what cases does the Department deem it relevant to interrogate a citizen about their religious or political beliefs? These are legitimate questions that need to be answered.

Privacy advocates have attempted to use the Freedom of Information Act (FOIA) to obtain the DHS policy with respect to questioning about religious and political beliefs and searches of handwritten materials or electronic equipment such as telephones, personal electronic devices, and computers. The DHS has not been forthcoming with this policy information and advocates have now sued to compel the agency's response. Americans are much more likely to tolerate security measures when they know that the basis for them is legitimate, and when their execution is reasonable. If a Federal agency bases its policy on racial or religious profiling, in the absence of any reasonable, particularized suspicion and contrary to our values, Americans are right to ask questions and demand justification.

I hope that today's hearing will help us understand the implications of these practices on privacy and civil liberties interests, as well as on business and economic concerns. Americans want security, but they also want a Federal Government that respects the diversity and privacy of its citizens.

#####

MUBANY
Muslim Bar Association of New York

P.O. Box 1171, New York, New York 10013 – www.muslimbarny.org

July 9, 2008

The Honorable Russell D. Feingold
Chairman
U.S. Senate Committee on the Judiciary
Subcommittee on The Constitution
224 Dirksen Senate Office Building
Washington, D.C. 20510

RE: June 25, 2008 Hearing on Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel

Dear Senator Feingold:

We, the Muslim Bar Association of New York, write to this letter to express our concern about the United States Customs and Border Protection Agency's (CBP) practice of conducting invasive border searches and interrogations. As a professional organization of Muslim lawyers living and practicing in the same jurisdiction as some of the nation's busiest ports, we have a strong interest in this issue and we thank the Subcommittee for receiving comments and testimony on this important matter. We respectfully request that this letter be included in the Subcommittee's record.

The CBP's invasive border searches & interrogations – as outlined during the Subcommittee's hearings on June 25, 2008 – are illustrative of a troubling disregard for individual liberty and personal privacy. The individual and subjective discretion CBP officials employ to conduct searches and interrogations at the border opens the door to racial and religious profiling. Such profiling offends numerous constitutional principles, including Due Process and Equal Protection. The Fourth Amendment does not permit excessive and intrusive searches merely because technology is rapidly advancing. Additionally, as lawyers and as members of America's Muslim community, we are keenly aware of how border interrogations that focus on an individual's religious beliefs or on an individual's travel companions no doubt threaten that individual's First Amendment rights.

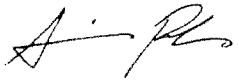
The CBP's invasive searches and interrogations are also counterproductive because they result in an inefficient and ineffective use of scarce resources. Excessive resources are spent on scrutinizing and potentially alienating law-abiding Americans at the expense of other more effective security measures. As citizens, we are concerned that individuals for whom the security screening is intended could circumvent the system by consciously avoiding profiles that triggers scrutiny.

Instead of relying upon ineffective and offensive profiling mechanisms, CBP officials should rely upon a "reasonable suspicion" standard. By doing so, the CBP can bypass superficial considerations and instead focus on individuals who pose legitimate threat.

In the interests of protecting individuals' civil rights at U.S. borders, the CBP and the Department of Homeland Security should provide transparent data on border searches and interrogations. We understand that both agencies have refused to respond in any meaningful way to Freedom of Information Act requests for such information. As such, we respectfully ask that Congress: 1) commission a GAO report and 2) impose reporting requirements covering (a) aggregate statistical data, along with (b) case-specific reports documenting the retention and destruction of electronic data seized from travelers. Such information may assist Congress and the public with understanding how we can improve our border security in a way that protects the rights of Americans while keeping them safe from harm.

If you have any questions or if you require additional information, please do not hesitate to contact me at president@muslimbarny.org. You can also learn more about the Muslim Bar Association of New York by visiting our website at www.muslimbarny.org.

Respectfully,



Asim Rehman, Esq.
President
Muslim Bar Association of New York

May 1, 2008

Chairman Patrick J. Leahy
Ranking Member Arlen Specter
United States Senate
Committee on the Judiciary

Dear Chairman Leahy and Ranking Member Specter:

We are writing to urge the Senate Committee on the Judiciary to hold hearings on the Department of Homeland Security's practice of searching and seizing Americans' digital information and electronic devices at U.S. borders. We also urge you to consider legislation to prevent abusive search practices by border agents and protect all Americans against suspicionless digital border inspections. In a free country, the government cannot have unlimited power to read, seize, store and use all information on any electronic device carried by any traveler entering or leaving the nation.

This issue is particularly critical in light of the Ninth Circuit Court of Appeals' recent decision in *United States v. Arnold*, which permits customs officials to search laptop computers at the border without any suspicion or cause.[1] Despite reassurances that border patrol agents are well trained and supervised,[2] the public has been unable to learn through open government laws which policies and procedures Customs and Border Patrol (CBP) has in place to protect travelers against arbitrary or abusive searches. Therefore, Congress must exercise oversight to ensure that border searches are not overly invasive or discriminatory, and establish appropriate safeguards to protect any information collected and maintained by the government.

- **This concern is real**. The press has reported disturbing stories of travelers whose electronic devices were seized by the government as they crossed U.S. borders. Ellen Nakashima, *Clarity Sought on Electronic Searches*, WASHINGTON POST, Feb. 7, 2008, at A1. In each case, the traveler, a member of an ethnic minority, was detained, and his or her digital device taken by a government agent. In two cases, the digital devices were password-protected corporate laptops.

- **The government's "profiles" are arbitrary**. CBP has said that "suspicious" travelers include men traveling from Asia between the ages of 20 and 59, a

[1] *United States v. Arnold*, No. 06-50581, 2008 U.S. App. LEXIS 8590 (9th Cir. Apr. 21, 2008).

[2] "Customs keeps track of the border searches its agents conduct, including the reasons for the searches. This administrative process should help minimize concerns that gas tank searches might be undertaken in an abusive manner." *United States v. Flores-Montano*, 541 U.S. 149, 156 (2004) (Breyer, J., concurring).

category so broad as to be meaningless. *See* Editorial, *Looking into Laptops*, LOS ANGELES TIMES, Nov. 11, 2006.

• **The government will not tell the public what it is actually doing.** Numerous Freedom of Information Act requests have been filed to learn more about the government's policies and procedures for conducting electronic border searches. Unfortunately, agencies have been slow to respond and have refused to turn over a great deal of important information. This is particularly troubling when CBP is solely responsible for protecting travelers' civil liberties at the border.

• **Everyone's privacy and security are at stake.** Your information may be compromised even if you don't travel yourself. The Association of Corporate Travel Executives has warned its members to consider the implications of traveling with confidential corporate information such as personnel records. American law firms that represent companies with offices in other countries are also concerned about their clients' confidences. Any individual's laptop can hold vast amounts of personal information such as financial records, confidential information related to business dealings and client relationships, and communications with friends, family and business associates. Allowing the government unchecked access to such information not only violates privacy and security, but also chills free expression.

The Fourth Amendment protects us all against unreasonable government intrusions. But this guarantee means nothing if CBP can arbitrarily search and seize our digital information at the border and indefinitely store and reuse it. We urge the Committee to hold swift hearings on the Department of Homeland Security's border search practices and consider legislative action to ensure that Americans' electronic devices are not subject to abusive, arbitrary or suspicionless searches at the borders.

For additional information, please feel free to contact Electronic Frontier Foundation Senior Staff Attorney Lee Tien at (415) 436-9333 x. 102.

Sincerely,

9/11 Research Project
American Association of University Professors
American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Immigration Lawyers Association
Asian Law Caucus
Association of Corporate Travel Executives
Professor Matt Blaze, University of Pennsylvania
Business Travel Coalition
Center for Democracy and Technology
Citizen Outreach Project
Defending Dissent Foundation
Whitfield Diffie (Sun Microsystems, for informational purposes only)
Electronic Frontier Foundation
Electronic Privacy Information Center
EnviroJustice
Equal Justice Alliance
Fairfax County Privacy Council
Feminists for Free Expression
Lauren Gelman, Executive Director, Stanford Law School Center for Internet and Society
Identity Project

Center for Digital Democracy
Susan Landau (Sun Microsystems, for informational purposes only)
Liberty Coalition
Minnesota Coalition on Government Information
The Multiracial Activist
Muslim Advocates
National Association of Criminal Defense Lawyers
National Center for Transgender Equality
National Coalition Against Censorship
PEN American Center
National Workrights Institute
OpenTheGovernment.org
People For the American Way
Republican Liberty Caucus
Professor Ronald L. Rivest, MIT
Professor Aviel D. Rubin, Johns Hopkins University
Rutherford Institute
Professor Fred B. Schneider, Cornell University
Bruce Schneier
U.S. Bill of Rights Foundation
The Woodhull Freedom Foundation

June 20, 2008

The Honorable Patrick J. Leahy
The Honorable Arlen Specter
United States Senate
Committee on the Judiciary
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Specter:

We write to urge the U.S. Senate Committee on the Judiciary to hold hearings on interrogations and searches by the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) of law-abiding Americans returning from international travel. These practices raise concerns about civil liberties across a range of contexts.

Many of the undersigned organizations recently urged Congress to hold hearings on CBP's routine, suspicionless searches of laptops and other personal belongings.[1] We now write to urge you to also (1) address in your oversight the full range of abusive CBP practices, including invasive interrogations, and their impact on the rights of Americans at the border; and (2) consider legislation to prevent invasive interrogations by CBP agents and to protect law-abiding Americans against routine scrutiny.

In addition to suspicionless searches that offend the Fourth Amendment, Americans returning home from abroad also face arbitrary questions from authorities that chill the exercise of core First Amendment freedoms. Specifically, Americans from all walks of life have been interrogated by CBP agents about their political views and activities; religious beliefs and practices; and associations with friends and relatives.

- **This problem is pervasive**. Civil rights groups have received numerous complaints from travelers who, upon re-entry to the U.S., were subjected to invasive questions. The press has also reported disturbing stories of CBP agents subjecting even U.S. citizens traveling *within* the U.S. to "aggressive questioning."[2]

    1. For instance, a religious scholar born in the U.S. is subjected to scrutiny routinely when returning from frequent international travel. CBP agents at Newark International Airport have interrogated him several times about the contents of his lectures, the places where he has lectured, and even the mosques in which he has prayed. In addition, CBP agents at Houston Intercontinental Airport have also interrogated him about his views of particular religious doctrines. Further, CBP agents at various locations have on several occasions photocopied his lecture notes and reviewed files on his computer, and agents at the Niagara Falls border crossing also seized and recorded data from his cell phone before interrogating him about his relationships with individuals who appeared in it. He has asked authorities both informally and formally about the basis for the apparent suspicion he has received. Citing national security

---

[1] *See* Letter from ACLU, Electronic Frontier Foundation et al. to Chairman Leahy and Ranking Member Specter (May 1, 2008), *available at* http://www.eff.org/press/archives/2008/05/01/border-search-open-letter; *U.S. v. Arnold*, 2008 U.S. App. LEXIS 8590 (9th Cir., April 21, 2008).

[2] *See, e.g.*, Sara Jean Green, *Border Patrol "spot checks" on ferries provoke outrage in San Juan Islands*, SEATTLE TIMES (April 22, 2008).

concerns, however, authorities have denied him any explanation for the scrutiny he continues to endure, or guidance about how to relieve it. Ironically, this U.S. citizen is currently pursuing a doctoral degree in Islamic studies at Yale University, has been cited by press outlets including *The Houston Chronicle* and *The Washington Post* as an expert on mainstream Islam and the integration of Muslims in the U.S., and has been consulted by government officials at agencies including the National Counterterrorism Center and the Department of State.

2. A lawyer in California was interrogated by CBP agents at San Francisco International Airport upon her return to the U.S. from a trip to visit overseas relatives. Upon establishing her citizenship status, she thoroughly answered initial questions about her travels and identity. Nevertheless, without any reason to believe that this U.S. citizen was carrying prohibited items or was otherwise engaged in unlawful activity, the CBP agent arbitrarily insisted on searching her luggage, seized her digital camera and reviewed the images — reflecting pictures from her travel with her family, as well as various photos taken in the United States prior to her travel. The agent interrogated her about the identities of the people in her travel photos, their location, and her relationships to them. The CBP agent then posed questions about her political views of candidates in the 2008 presidential election.

3. An engineer in the information technology sector was detained for several hours, searched and interrogated at San Francisco International Airport after returning from an overseas business trip that included a visit with family members. CBP agents seized and searched his checkbook, asked questions about his donations to particular charitable and religious organizations, and also investigated his associations with particular community leaders. The agent demonstrated familiarity with the organizations and their leaders — none of whom have been designated by the federal government as targets of scrutiny. After seizing (and ultimately confiscating) the traveler's cell phone, the agent advised him that he "would be in big trouble" if a search of its contents revealed the names of particular leaders of some organizations to which he had donated. This traveler's cell phone was ultimately returned, in a broken and inoperable condition, five months after this incident – around the same time that he became a naturalized U.S. citizen.

- **Invasive interrogation offends several core constitutional rights**. CBP practices described in this letter burden substantive constitutional rights, including the Fourth Amendment guarantee against unreasonable searches and seizures and the First Amendment freedom to maintain political views, religious views and personal associations without inviting government scrutiny.

- **The privacy, security and liberty of law-abiding Americans are at stake**. Even the privacy of Americans who are not themselves traveling across the border stands at risk. Invasive interrogation about individuals' relationships with family and friends burdens the First Amendment right of association. Similarly, routine searches of digital cameras, cellular phones and handwritten notes place at risk of potential scrutiny the various subjects of a traveler's photos, cell phone contacts, or even people merely referenced in a traveler's private personal diary. Finally, known scrutiny of individuals on the basis of their participation in religious communities chills third parties from exercising their constitutional right to participate in those communities.

- **The government's "profiles" are arbitrary, opaque, and demonstrably inaccurate, and they violate prior guidance from the Executive Branch.** CBP has confirmed the use of profiles so broad as to be meaningless. For instance, travelers deemed presumptively "suspicious" include all men between the ages of 20 and 59 traveling from Asia.[3] Similarly, CBP training materials suggest "it is permissible and indeed advisable to consider an individual's connections to countries that are associated with significant terrorist activity," which could essentially entail "targeting people because they are Arab or Muslim," absent any potentially protective policies.[4] This guidance runs counter to the President's pledge to end racial profiling[5] and highlights why previous guidance issued by the Department of Justice remains inadequate to protect Americans from arbitrary scrutiny on the basis of their race, religion or ethnicity.[6]

- **The government refuses to disclose its actual practices.** Despite informal requests, as well as formal requests under the Freedom of Information Act, agencies have refused to disclose meaningful information about any potential policies and procedures for interrogations, searches or seizures at the border. Moreover, as the press has reported, "the factors agents use to single out passengers are not transparent, and travelers generally have little access to the data to see whether there are errors."[7]

- **The CBP's assertion of authority over returning travelers is *ultra vires*.** CBP agents are questioning travelers — including U.S. citizens — about matters well outside the agency's institutional purview.[8] Whether, when, how, and under what legal authority the agency's authority has expanded remains unknown to the public. Moreover, many of these questions would be impermissible to raise in other settings. For example, absent a warrant, an FBI agent would not be entitled to detain a citizen within the country in order to interrogate him or her about religious practices or donations to local houses of worship.

- **CBP's detentions, searches, seizures and interrogations are inherently coercive.** CBP's position at the border generally intimidates returning citizens, who are tacitly led to believe

---

[3] *See* Editorial, *Looking into Laptops*, LOS ANGELES TIMES, Nov. 11, 2006.
[4] Ellen Nakashima, *Clarity Sought on Electronics Searches*, WASHINGTON POST (February 7, 2008).
[5] *See* President George W. Bush, *Memorandum for the Attorney General* (Feb. 27, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/02/20010228-1.html; The White House, *Record of Achievement: Fighting Crime* (noting that "Less than six weeks after taking office, President Bush called for an end to racial profiling in Federal law enforcement."), *available at* http://www.whitehouse.gov/infocus/achievement/chap16.html.
[6] *See* Dep't of Justice, *Justice Department Issues Policy Guidance to Ban Racial Profiling* (June 17, 2003), *available at* http://www.usdoj.gov/opa/pr/2003/June/03_crt_355.htm ("The racial profiling guidance bars federal law enforcement officials from engaging in racial profiling . . . . has been adopted by the President as executive policy for federal law enforcement, and governs all federal law enforcement activities . . . ."); *see also* Exec. Order No. 12,333, §2.4 ("Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad.").
[7] Nakashima, *supra* note 4.
[8] *See* 8 C.F.R. § 287.1 (2008).

that they must answer CBP questions in order to gain entry to the country. Travelers are rarely aware of their rights at the border, leaving them vulnerable to invasive interrogation by overzealous CBP officials eager to insinuate their authority.

Accordingly, Congress must exercise its oversight authority to ensure that border interrogations and searches respect the Fourth Amendment and do not chill the exercise of beliefs and activities protected by the First Amendment. CBP should not be allowed to continue exceeding its authority by leveraging the inherently coercive setting of interrogations at the nation's border to subject law-abiding Americans to questions that violate their rights.

We urge the Committee to hold swift hearings on CBP and DHS border search practices, and to consider legislative action to protect law-abiding Americans from arbitrary and invasive interrogation when returning home from abroad.

For additional information, please contact Muslim Advocates Counsel Shahid Buttar at (415) 692-1512 or Shahid@MuslimAdvocates.org.

Respectfully submitted,

Asian Law Caucus
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
Association of Physicians of Pakistani-descent of North America
Bill of Rights Defense Committee
Center for National Security Studies
Defending Dissent Foundation
Electronic Frontier Foundation
Fairfax County Privacy Council
The Freedom and Justice Foundation
Friends Committee on National Legislation
Liberty Coalition
NAACP Legal Defense Fund, Inc.
Mexican-American Legal Defense and Educational Fund
MAS Freedom
Muslim Advocates
Muslim Bar Association of New York
Muslim Consultative Network
National Lawyers Guild
National Council of La Raza
People for the American Way
Privacy Times
Privacy Journal
South Asian Americans Leading Together
Sikh Coalition
Unitarian Universalist Service Committee
U.S. Bill of Rights Foundation

Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel
United States Senate Committee on the Judiciary,
Subcommittee on the Constitution, Civil Rights and Property Rights
June 25, 2008

Statement of Nathan A. Sales
Assistant Professor of Law, George Mason University School of Law

Chairman Feingold, Ranking Member Brownback, and Members of the Subcommittee, thank you for inviting me to testify on this important issue. My name is Nathan Sales, and I am a law professor at George Mason University School of Law, where I teach national-security law and administrative law. Previously, I served at the United States Department of Homeland Security as the Deputy Assistant Secretary for Policy Development. Please understand that the views I will express are mine alone, and should not be ascribed to any past or present employer or client.

The gist of my testimony is as follows. Border searches of laptop computers and other electronic devices implicate a range of compelling, and sometimes competing, interests. Those interests include the government's paramount need to detect terrorists crossing our borders and to combat child pornography, as well as law-abiding travelers' equally weighty interest in maintaining their personal privacy. A series of Supreme Court cases has held that "routine" border searches – i.e., searches of property – need not be preceded by any individualized suspicion whatsoever. These searches satisfy the Fourth Amendment's reasonableness requirement simply by virtue of the fact that they occur at the border. The consensus among lower federal courts is that a laptop search counts as "routine"; officers therefore don't need to have reasonable suspicion before inspecting a particular traveler's computer. Finally, while the Fourth Amendment imposes few restrictions on laptop searches, policymakers might wish to implement other safeguards that supplement these relatively modest constitutional protections.

I. The Competing Interests of Laptop Searches.

The government has an interest of the highest order in incapacitating terrorists who may be trying to enter this country. The 9/11 Commission reminded us that, for terrorists, the ability to travel is "as important as weapons."[1] Each time an al Qaeda operative boards a plane or crosses a border represents an opportunity to detect and capture him. One way to do so is to inspect the belongings travelers are carrying when they land, including their computers.

Consider Zacarias Moussaoui, the convicted 9/11 conspirator and al Qaeda operative. Moussaoui evidently stored incriminating data on his laptop computer, including information about crop-dusting aircraft and wind patterns.[2] If investigators had found this data on

[1] THE 9/11 COMMISSION REPORT 384 (2004).

[2] *See* Philip Shenon, *Threats and Responses: The Judiciary; Congress Criticizes F.B.I. and Justice Department Over Actions Before Secret Wiretap Court*, N.Y. TIMES, Sept. 11, 2002, at A18.

Moussaoui's laptop when he arrived in the United States, it's possible they might have begun to unravel his ties to al Qaeda.[3] More recently, in 2006, a laptop search at Minneapolis-St. Paul airport helped U.S. Customs and Border Protection officers detect a potentially risky traveler. Once he was referred to secondary inspection, CBP discovered that he had a manual on how to make improvised explosive devices, or IEDs – a weapon of choice for terrorists in Afghanistan and Iraq. Inspecting the passenger's computer, officers also found video clips of IEDs being used to kill soldiers and destroy vehicles, as well as a video on martyrdom.[4]

Terrorism is not the only threat laptop searches can detect. Inspections of international travelers' computers also have proven instrumental in the government's efforts to combat child pornography and even ghastlier forms of child exploitation. In fact, there have been eleven federal decisions examining the scope of CBP's authority to search laptops at the border, and every single one has involved child pornography.

United States v. Irving[5] is chillingly representative. The defendant in that case, Stefan Irving, used to be the chief pediatrician for a school district in New York, but his license to practice medicine was stripped after a 1983 conviction for "attempted sexual abuse in the first degree of a seven-year old boy."[6] On May 27, 1998, Irving flew from Mexico to Dallas-Fort Worth International Airport. The purpose of his trip to Mexico had been to visit "a guest house that served as a place where men from the United States could have sexual relations with Mexican boys"; the defendant "preferred prepubescent boys, under the age of 11."[7] After Irving's flight arrived, customs officers searched his luggage and found "children's books and drawings that appeared to be drawn by children," as well as "a disposable camera and two 3.5 inch computer diskettes." The disks were analyzed and found to contain "[i]mages of child erotica."[8]

Unfortunately, Stefan Irving is far from an anomaly. A 2000 search at the U.S.-Canada border uncovered a computer and some 75 disks containing child pornography. One of the disks included "a home-movie of [the defendant] fondling the genitals of two young children. The mother of the two children later testified that [the defendant] was a family friend who had babysat her children several times in their Virginia home."[9] In 2006, a border search of a vehicle at Bar Harbor, Maine turned up a laptop with numerous images of child pornography; officers also found "children's stickers, children's underwear, children's towels or blankets with super heroes printed on them," as well as "12-15 condoms" and "a container of personal lubricant."[10]

---

[3] For a discussion of the FBI's failure to obtain judicial authorization to search Moussaoui's laptop after his August 16, 2001 arrest, see Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951, 957-72 (2003).

[4] *See* Remarks of Stewart A. Baker, Assistant Secretary for Policy, United States Department of Homeland Security, at the Center for Strategic and International Studies, Dec. 19, 2006.

[5] 452 F.3d 110 (2d Cir. 2006).

[6] *Id.* at 114.

[7] *Id.* at 115.

[8] *Id.*

[9] United States v. Ickes, 393 F.3d 501, 503 (4th Cir. 2005).

[10] United States v. Hampe, Crim. No. 07-3-B-W, 2007 WL 1192365, at *2 (D. Me. April 18, 2007).

Last year, at Del Rio, Texas, a border search of an external hard drive revealed "101,000 still images depicting child pornography" and "890 videos depicting pornographic images of children."[11]

While the government's interest in combating terrorism and child exploitation are significant indeed, the other side of the ledger has weighty interests of its own. Border searches of law-abiding travelers' laptop computers and other electronic devices have the potential to intrude on legitimate privacy interests in unprecedented ways. "Individuals have a basic interest in withdrawing into a private sphere where they are free from government observation."[12] Privacy concerns are particularly acute when the traveler is a United States citizen, since courts generally recognize that Americans have stronger privacy interests under the Constitution than aliens who are only visiting this country temporarily.[13]

Laptops can contain vast amounts of information. An 80-gigabyte hard drive is capable of storing the equivalent of 40 million printed pages. That's equal to "the amount of information contained in the books on one floor of a typical academic library."[14] Moreover, the type of data stored on a laptop can be intensely personal. A computer might contain digital photographs from the owner's vacation, an address book listing all of the owner's contacts, thousands of emails sent and received over the course of years, and so on; a laptop can function simultaneously as a photo album, Rolodex, and correspondence file. In addition to personal data, business travelers may keep trade secrets and other proprietary information on their laptops. And lawyers' computers might have materials covered by the attorney-client privilege. For these reasons, Professor David Cole of Georgetown University Law Center has likened computers to houses: "What a laptop records is as personal as a diary but much more extensive. It records every Web site you have searched. Every email you have sent. It's as if you're crossing the border with your home in your suitcase."[15]

II. The Supreme Court's Border-Search Precedents.

The Fourth Amendment's prohibition on unreasonable searches and seizures applies differently at the border than it does within the United States. While the government ordinarily must establish probable cause and obtain a warrant from a judge before conducting a search, the Supreme Court has carved out an exception for border searches. "Since the founding of our Republic," the government has had "plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to prevent the introduction of

---

[11] United States v. McAuley, No. DR-07-CR-786(1)-AML, 2008 WL 2387979, at *2 (W.D. Tex. June 6, 2008).

[12] Nathan Alexander Sales, *Secrecy and National Security Investigations*, 58 ALA. L. REV. 811, 823 (2007).

[13] *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 261-65 (1990) (holding that a Mexican national could not invoke the Fourth Amendment's guarantee against unreasonable searches and seizures to challenge a warrantless search by federal agents of his residences in Mexico, in part because he was not within the "class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community").

[14] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005)

[15] *Quoted in* Ellen Nakashima, *Clarity Sought on Electronics Searches*, WASH. POST, Feb. 7, 2008, at A01.

contraband into this country."[16] In fact, just two months before it sent what would become the Fourth Amendment to the states for ratification, Congress enacted legislation granting customs officials "full power and authority" to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed."[17] This power to "require that whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry"[18] derives from the "inherent authority" of the United States "as sovereign" to "protect . . . its territorial integrity."[19]

There are two kinds of border searches: "routine" and "non-routine." Routine searches – i.e., searches of cargo, luggage, and other property – "are not subject to any requirement of reasonable suspicion, probable cause, or warrant."[20] For routine inspections, officers don't need to have any suspicion whatsoever, reasonable or otherwise. The Fourth Amendment permits them to conduct "*suspicionless*" searches.[21] This is not to suggest that the Fourth Amendment's reasonableness requirement doesn't apply at the border. It does. But border searches are deemed "reasonable simply by virtue of the fact that they occur at the border."[22]

Non-routine border searches are subject to the somewhat more exacting reasonable-suspicion standard. Before conducting this kind of inspection, officers must have some particularized basis for suspecting that the person to be searched is engaged in wrongdoing, such as carrying contraband.[23] So what counts as a non-routine search? The Supreme Court has indicated that invasive searches of the body are non-routine – for example, strip searches, body-cavity searches, and involuntary x-ray searches.[24] The reasons for requiring at least "some level of suspicion" before performing "highly intrusive searches of the person" are the "dignity and privacy interests of the person being searched."[25] Searches of the body are more invasive than

---

[16] United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

[17] Act of July 31, 1789, c. 5, § 24, 1 Stat. 29, *quoted in* United States v. Ramsey, 431 U.S. 606, 616 & n.12 (1977). The Act's modern descendent is 19 U.S.C. § 1581(a). It provides:

> Any officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States or within the customs waters . . . and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board, and to this end may hail and stop such vessel or vehicle, and use all necessary force to compel compliance.

[18] Torres v. Puerto Rico, 442 U.S. 465, 473 (1979).

[19] United States v. Flores-Montano, 541 U.S. 149, 153 (2004).

[20] *Montoya de Hernandez*, 473 U.S. at 538; *see also id.* at 551 (Brennan, J., dissenting) (agreeing that "thorough searches of [travelers'] belongings . . . do not violate the Fourth Amendment").

[21] *Flores-Montano*, 541 U.S. at 154 (emphasis added).

[22] *Ramsey*, 431 U.S. at 616; *see also id.* at 619 ("Border searches . . . have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside."); *id.* at 620 ("It is their entry into this country from without it that makes a resulting search 'reasonable.'").

[23] *See, e.g.*, United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006); United States v. Rivas, 157 F.3d 364, 367 (5th Cir. 1998).

[24] *See Montoya de Hernandez*, 473 U.S. at 541 n.4.

[25] *Flores-Montano*, 541 U.S. at 152.

searches of belongings, and the Court therefore insists that officers have a measure of individualized suspicion before conducting them.

III. Laptop Searches Under the Fourth Amendment.

The question then becomes whether a border laptop inspection is a routine search that can be performed without any particularized suspicion at all, or a non-routine search that must be justified by reasonable suspicion. The Supreme Court has never addressed the question. But a consensus is emerging among the lower federal courts that laptop inspections are routine searches for which reasonable suspicion is unnecessary.

By my count, there have been eleven federal decisions applying the Supreme Court's border-search precedents to laptop computers and other electronic storage devices. Seven of the eleven hold or imply that CBP may search laptops at the border with no particularized suspicion at all: The Ninth Circuit (twice), Fourth Circuit, Eastern District of Pennsylvania, Western District of Texas, District of Maine, and Southern District of Texas.[26] (The Third Circuit has hinted, in a case involving an inspection of a traveler's videotape, that it takes the same view.[27]) Three courts – the Second Circuit, Fifth Circuit, and District of Minnesota – dodged the question. The officers in those cases had reasonable suspicion to search the laptops and the courts therefore found it unnecessary to decide whether suspicionless searches were permissible.[28] Other than a single California district court that was reversed on appeal,[29] no court has held that customs officers must have reasonable suspicion before they search a laptop. No court has held that probable cause is needed to conduct a laptop search at the border. And no court has held that customs must obtain a warrant before examining a laptop.

My sense is that the Supreme Court is unlikely to disturb this lower-court consensus. For starters, the Court on at least two prior occasions has declined invitations to extend the more rigorous standards for invasive body searches into the realm of property searches. In *United States v. Ramsey*, the Court upheld a suspicionless border search of international mail, rejecting the notion that "whatever may be the normal rule with respect to border searches, different

---

[26] *See* United States v. Arnold, 523 F.3d 941, 948 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 505 & n.1 (4th Cir. 2005); United States v. Bunty, Crim. No. 07-641, 2008 WL 2371211, at *3 (E.D. Pa. June 10, 2008); United States v. McAuley, No. DR-07-CR-786(1)-AML, 2008 WL 2387979, at *4-6 (W.D. Tex. June 6, 2008); United States v. Hampe, Crim. No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. April 18, 2007); United States v. Roberts, 86 F. Supp. 2d 678, 688-89 (S.D. Tex. 2000), *aff'd*, 274 F.3d 1007 (5th Cir. 2001); *cf.* United States v. Romm, 455 F.3d 990, 997 n.11 (9th Cir. 2006) (reading Supreme Court caselaw as "suggest[ing] that the search of a traveler's property at the border will always be deemed 'routine,'" but declining to resolve the issue since the defendant waived his argument).

[27] *See* United States v. Linarez-Delgado, 259 Fed. Appx. 506, 507-08 (3d Cir. 2007) (emphasizing that customs officials may "conduct routine searches and seizures for which the Fourth Amendment does not require a warrant, consent, or reasonable suspicion," including searches of "[d]ata storage media and electronic equipment, such as films, computer devices, and videotapes").

[28] *See* United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006); United States v. Roberts, 274 F.3d 1007, 1012 (5th Cir. 2001); United States v. Furukuwa, Crim. No. 06-145 (DSD/AJB), 2006 WL 3330726, at *1 (D. Minn. Nov. 16, 2006).

[29] *See* United States v. Arnold, 454 F. Supp. 2d 999 (C.D. Cal. 2006), *rev'd*, 523 F.3d 941 (9th Cir. 2008).

considerations, requiring the full panoply of Fourth Amendment protections, apply to international mail."[30] Likewise, in *United States v. Flores-Montano*, a unanimous Court denied that border searches involving the disassembly of vehicles required reasonable suspicion.[31] The Court appears to be drawing something of a bright-line rule: Invasive searches of the body might require reasonable suspicion, but searches of property – even quite sensitive types of property, like letters – do not.[32] As property, a laptop falls on the other side of the line.

The Court might be disinclined to establish a reasonable-suspicion requirement for laptop searches for another reason: Doing so would mean that the level of legal protection for messages, photos, and other data would vary based on whether they are kept in digital or physical format. Governing caselaw permits customs officers to conduct suspicionless border searches of mail,[33] address books,[34] photo albums,[35] and similar items, even though each can contain personal information of extreme sensitivity. A laptop computer is essentially a digitized version of a correspondence file, address book, and photo album, all in a single container. I suspect the Supreme Court would be reluctant to hold that data stored electronically is entitled to stronger privacy protections than the very same data would be if stored on paper.

Indeed, *Ramsey* hinted as much. In that case, the Court stressed that "there is nothing in the rationale behind the border-search exception which suggests that [a letter's] mode of entry will be critical." It went on to conclude that "no different constitutional standard should apply simply because the envelopes were mailed not carried. The critical fact is that the envelopes cross the border and enter this country, not that they are brought in by one mode of transportation rather than another"[36] Just as the manner in which envelopes are transported is irrelevant to the privacy protections their owners enjoy, so too the scope of privacy at the border should not depend on the fortuity that a traveler happens to store his personal information in the digital world and not the analog one. The mere fact of computerization shouldn't make a difference.[37]

Finally, I don't anticipate that the Court will be persuaded by efforts to liken laptop computers to homes. The reason the home has enjoyed uniquely robust privacy protections in the Anglo-American legal tradition is because it is a sanctuary into which the owner can withdraw from the government's watchful eye. "[A] man's house is his castle," and "'[t]he

---

[30] 431 U.S. 606, 619-20 (1977).

[31] 541 U.S. 149, 154-55 (2004).

[32] Of course, the Court has indicated that some searches of property are so destructive that they require particularized suspicion, and that a search might be unreasonable because it is carried out in a particular offensive manner. *See id.* at 155-56, 155 n.2. Neither of those exceptions seems applicable to an ordinary laptop search.

[33] *See, e.g.*, United States v. Ramsey, 431 U.S. 606, 619-23 (1977).

[34] *See, e.g.*, United States v. Soto-Teran, 44 F. Supp. 2d 185, 191-92 (E.D.N.Y. 1996), *aff'd*, 159 F.3d 1349 (2d Cir. 1998).

[35] *See, e.g.*, United States v. Ickes, 393 F.3d 501, 503 (4th Cir. 2005).

[36] *Ramsey*, 431 U.S. at 620.

[37] *See* United States v. McAuley, No. DR-07-CR-786(1)-AML, 2008 WL 2387979, at *5 (W.D. Tex. June 6, 2008) ("The fact that a computer may take such personal information and digitize it does not alter the Court's analysis.").

poorest man may in his cottage bid defiance to all the forces of the Crown.'"[38] Crossing an international border is in many ways the opposite of this kind of withdrawal. Rather than concealing oneself from the government, one is voluntarily presenting oneself to the government for inspection and permission to enter the country. One's expectation of privacy is considerably lower in those circumstances than when one is at one's residence. "[A] port of entry is not a traveler's home."[39]

Practically speaking, it ultimately may not matter whether courts allow suspicionless laptop searches or insist on reasonable suspicion. Secretary of Homeland Security Michael Chertoff has indicated that, regardless of whether the Fourth Amendment allows suspicionless searches, "as a matter of practice, we only do it where there's a reasonable suspicion."[40] To see why that might be so, it helps to have a basic understanding of how CBP processes travelers when they arrive in the United States. An inbound traveler will undergo a brief interview with a CBP officer to establish identity and entitlement to enter the country; this is known as "primary" inspection. Most people are admitted without further scrutiny, but suspicious travelers are referred to "secondary" inspection for more detailed questioning and searches. Sometimes people are sent to secondary because officers think they look nervous. Sometimes they're referred because their answers are evasive. Sometimes they're referred because of a hit in CBP's Automated Targeting System – a computerized system that matches travelers' personal information against government databases of known and suspected terrorists, criminals, and so on. A referral to secondary conceivably could be enough to establish reasonable suspicion, especially a referral based on an ATS hit.[41] If so, whether a laptop search is routine or non-routine might not matter much at all.

IV. Policy Considerations.

The Fourth Amendment imposes relatively weak constraints on the ability of CBP officers to perform laptop searches at the border, but the Constitution is not the only possible source of privacy protections. Policymakers at the Department of Homeland Security might consider implementing a number of safeguards that go beyond what the Fourth Amendment requires.

---

[38] Miller v. United States, 357 U.S. 301, 307 (1958) (citations omitted); *see also* Wilson v. Layne, 526 U.S. 603, 610 (1999) (invoking the "centuries-old principle of respect for the privacy of the home"); Minnesota v. Carter, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) ("[I]t is beyond dispute that the home is entitled to special protection as the center of the private lives of our people.").

[39] United States v. Thirty-seven Photographs, 402 U.S. 363, 376 (1971); *cf. Ickes*, 393 F.3d at 502 (upholding a suspicionless border search of a vehicle even though "Ickes's van appeared to contain 'everything he own[ed]'" (alteration in original)).

[40] Testimony of Michael Chertoff, Secretary, United States Department of Homeland Security, Before the United States Senate Committee on the Judiciary, Apr. 2, 2008.

[41] *See, e.g.*, United States v. Bunty, Crim. No. 07-641, 2008 WL 2371211, at *3 & n.7 (E.D. Pa. June 10, 2008) (suggesting that an ATS hit established reasonable suspicion); *McAuley*, No. DR-07-CR-786(1)-AML, 2008 WL 2387979, at *5 n.7 (same); United States v. Furukuwa, Crim. No. 06-145 (DSD/AJB), 2006 WL 3330726, at *5 (D. Minn. Nov. 16, 2006) (same).

As a matter of first principles, CBP should provide the public with as much information about its laptop searches as is consistent with operational necessity. "[I]n the American constitutional system, transparency and openness is the general rule to which secrecy is the occasional exception."[42] Transparency would help ensure that any abuses of CBP's laptop-search powers are corrected, and thus contribute to the searches' perceived legitimacy. Of course, certain operational details may need to be kept under wraps to prevent the sources and methods the government uses to gather information from being compromised.[43] In those cases, CBP could provide classified briefings to the appropriate Members of Congress in lieu of full public disclosure.

CBP also might formalize the standards it uses to pick travelers for laptop searches. For instance, are people selected randomly? On the basis of previous travel history? The manner in which they paid for their airline tickets? Tips from other government agencies about particular passengers? CBP officers' observations about travelers' demeanor? Some combination of factors? These standards would help provide assurances to people who are asked to undergo laptop inspections that they were selected due to legitimate law-enforcement or intelligence considerations, and not on the basis of impermissible criteria such as race or religion. Again, it must be stressed that CBP should not reveal too much about the factors it uses to select passengers for laptop searches. Doing so could provide terrorists, child pornographers, and other criminals with a roadmap for avoiding detection.[44]

Third, the government should consider guidelines to govern the amount of time it takes to complete a laptop search. The longer an inspection lasts, the more it inconveniences the laptop's owner. Lengthier searches also increase the likelihood that officers who are hunting for contraband will, whether deliberately or by accident, start browsing through entirely innocent (and sensitive) computer files. It may not be practicable to establish a hard and fast rule that all laptop searches must be completed within, say, ninety minutes. But at a minimum, CBP could set goals to encourage effective yet speedy searches.

Fourth, the government ought to adopt standards on the retention and use of data gathered from laptop searches. If a search fails to uncover any criminal activity, CBP would be hard pressed to justify retaining any data from the passenger's computer. When, on the other hand, the government has an obvious need to keep copies of files – for example, if the data itself is contraband or is evidence of crime – it should strictly enforce policies that limit employees' access to the data and punish those who retrieve it without permission. A related point: CBP should take special care to see that trade secrets, privileged correspondence, and other sensitive business information are handled with appropriate discretion, and that there are harsh penalties for employees who access or disclose such data without authorization.

---

[42] Sales, *supra* note 12, at 816.

[43] *See, e.g.*, CIA v. Sims, 471 U.S. 159, 167 (1985) (describing sources and methods as "the heart of all intelligence operations"); United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984) (emphasizing the "need to maintain the secrecy of lawful counterintelligence sources and methods" (quoting S. REP. NO. 95-701, at 15 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3983 (internal quotation marks omitted)).

[44] *Cf.* Detroit Free Press v. Ashcroft, 303 F.3d 681, 706 (6th Cir. 2002) ("This information could allow terrorist organizations to alter their patterns of activity to find the most effective means of evading detection.").

Finally, CBP should make and maintain detailed audit trails to ensure that any officer misconduct can be detected and punished. As Justice Breyer emphasized in a recent case involving border searches of automobiles, "Customs keeps track of the border searches its agents conduct, including the reasons for the searches. This administrative process should help minimize concerns that gas tank searches might be undertaken in an abusive manner."[45] It would have the same beneficial effect for laptop searches.

* * *

Mr. Chairman, thank you again for the opportunity to testify today. I would be happy to answer any questions you or the other Members of the Subcommittee might have.

[45] United States v. Flores-Montano, 541 U.S. 149, 156 (2004) (Breyer, J., concurring) (citation omitted)

Center for American Progress Action Fund

STATEMENT OF PROFESSOR PETER P. SWIRE
C. WILLIAM O'NEILL PROFESSOR OF LAW
MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY
SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS ACTION FUND

BEFORE

THE U.S. SENATE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS & PROPERTY RIGHTS

ON

"LAPTOP SEARCHES AND OTHER VIOLATIONS OF PRIVACY FACED BY AMERICANS RETURNING FROM OVERSEAS TRAVEL"

JUNE 25, 2008

Chairman Feingold, Ranking Member Brownback, and members of the Committee:

Thank you for the invitation to testify today on "laptop searches and other violations of privacy faced by Americans returning from overseas travel." In recent months I have become increasingly aware of what I consider a deeply flawed policy. The U.S. Customs and Border Patrol ("CPB") now takes the position that it can seize and copy the contents of a laptop or other computing device for a traveler entering the U.S., based simply on its authority to do traditional border searches.

The government seems to believe that, if they can open a suitcase at the border, then they can open a laptop as well. This simplistic legal theory ignores the massive factual differences between a quick glance into a suitcase and the ability to copy a lifetime of files from someone's laptop, and then examine those files at the government's leisure.

This issue has come into sharp focus since the April decision of the Ninth Circuit Court of Appeals in *U.S. v. Arnold*. That panel clearly ruled that CPB can seize a laptop computer at the border, and examine its contents, without any reasonable suspicion of unlawful activity. Affidavits in that case and other credible reports show that agents at the border are going further -- they are requiring travelers to reveal their passwords or encryption keys so that government agents can examine the full content of the laptop or other computing device.

Other witnesses today will go into depth about crucial objections to these laptop border searches, including constitutional prohibitions under the First and Fourth Amendments, ethnic profiling, and severe impact on commercial and individual travelers who are forced to reveal confidential records to the government.

My focus is different, drawing on my personal involvement in the encryption policy battles from a decade ago. My thesis is that laptop border searches bear a striking similarity to the federal encryption policy that was attempted during the 1990s but reversed in 1999. My testimony presents a brief history of these "crypto wars," as they were called. In particular, the testimony describes the so-called "Clipper Chip," where the government hoped to gain the encryption keys in advance for telecommunications devices. The testimony then examines eight precise analogies between the failed encryption policy of the 1990s and laptop border searches. For each of the eight critiques, the testimony explains how the critique applied to encryption policy and how the same argument applies to today's border searches:

1. Traditional legal arguments apply badly to new facts about computing
2. Government forces disclosure of encryption keys
3. Severe violation of computer security best practices
4. U.S. policy creates bad precedents that totalitarian and other regimes will follow
5. Severe harm to personal privacy, free speech, and business secrets
6. Disadvantaging the U.S. economy
7. Political coalition of civil liberties groups and business
8. Technical futility of U.S. policy

Since I became aware of the issue of laptop border searches I have spoken to an array of businesspeople, computer security experts, civil liberties advocates, and ordinary people who hear what the government is doing. The reaction has been uniform: "The government is doing *that*? They are just stopping people at the border, opening people's laptops and making copies of what's inside? It could happen to anyone, even if they've done nothing wrong? That is simply not right."

I hope today's hearing will be an important step toward curbing the current practices.

Background

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and a Senior Fellow with the Center for American Progress Action Fund. I live in the Washington, D.C. area. My education includes graduating summa cum laude from Princeton University and a J.D. from the Yale Law School.

From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that role, I was responsible for coordinating administration policy on public- and private-sector uses of personal information, and served as point of contact with privacy and data protection officials in other countries. During this time, along with many other activities, I participated in the process that resulted in a new administration policy for encryption in September, 1999. In 2000, at the request of Chief of Staff John Podesta, I chaired a 14-agency White House task force on how to update government surveillance laws for the Internet age.

Since leaving OMB, I have worked and written on a very wide variety of privacy and computer security issues. For instance, I testified before this Committee in 2007 about problems with the use of National Security Letters by the Federal Bureau of Investigation. I am Faculty Editor of the "Privacy Year in Review" issue of *I/S: A Journal of Law and Policy for the Information Age*, which is distributed to all members of the International Association of Privacy Professionals. My testimony and other writings appear at www.peterswire.net and www.americanprogress.org.

First and Fourth Amendment Analysis of Laptop Border Searches and Apparent Lack of Administrative Safeguards

This hearing was prompted in large measure by a decision by the 9th Circuit in April of this year, in the case of *Arnold v. U.S.*[1] Earlier federal cases had upheld laptop searches at the border, typically finding there had been "reasonable suspicion" of the individual, which means specific and articulable facts that led the government official to have a basis for carrying out the search. In the *Arnold* case, the district court found no "reasonable suspicion" for doing the search. The district court thus suppressed evidence discovered after a detailed search of the laptop. A Ninth Circuit panel reversed. It found, incorrectly in my view, that the CPB can do a comprehensive search of a laptop at the border without any reasonable suspicion of the individual.

Affidavits in the *Arnold* case and other reports indicate that, at least in some cases, CPB has seized a laptop at the border and returned it a week or more afterwards. The reports are that individuals are told, in addition, that they have to provide the government their passwords and encryption keys in order for the government to able to read the files in the computer. Failure to cooperate, travelers are told, is a basis for denying entry into the U.S.

I invite the Committee to consider how this sort of seizure, perhaps done without any individualized suspicion, would affect your work and your peace of mind -- having your laptop taken away from you, with no assurance you will get it back, and with the knowledge that the government could make a complete copy of the contents for analysis at its leisure.

I disagree with the Ninth Circuit, and agree with the position of the Electronic Frontier Foundation that the Fourth Amendment should be found to require at least a "reasonable suspicion" before doing an intrusive search of a laptop or other computing device at the border. The amicus brief filed in the *Arnold* appeal on behalf of EFF and the Association of Corporate Travel Executives lays out the legal arguments in considerable detail. Because I have reviewed these materials, and agree with them, I do not repeat the analysis here.

There are also serious issues under the First Amendment created by the seizure and copying of a person's laptop at the border. A laptop contains an enormous amount of expressive activity, potentially including confidential journalist notes, criticism of the Department of Homeland Security, and an almost unimaginable range of other content. The First Amendment aspects of privacy and searches have recently been examined by law professors Katherine Strandburg[2] and Daniel Solove,[3] and I commend those analyses to the Committee's attention.

Although I believe the Ninth Circuit decision is incorrect under the First and Fourth Amendments, **the Congress could take action to provide safeguards against overly intrusive searches** of laptops, other computing devices, and other examination of First Amendment-protected content at the border. **Similarly, Customs and Border Patrol, acting with the Privacy Officer and Civil Liberties**

Officer of the Department of Homeland Security, could create administrative safeguards to minimize the intrusiveness of searches of this sort of sensitive content. Because CPB has refused thus far to release any information about its practices, we do not know if any administrative safeguards are currently in place.

An important first step should be for the Department of Homeland Security to conduct a Privacy Impact Assessment of the procedures for conducting such searches. This sort of Assessment could address important issues such as: threshold for when content searches take place; protections against ethnic profiling and other improper targeting of travelers; minimization procedures for any data collected from searches; logging and audit procedures for such searches; and strict limits against any non-customs-related use of data collected from such searches. These sorts of administrative safeguards are an essential initial measure to control intrusive laptop searches and reassure lawful travelers that crossing the border will not be made an excuse for government surveillance of our entire universe of expressive activity.

Why Laptop Border Searches are Like the Failed Encryption Approach of the Clipper Chip Era

The main point of my testimony today is that laptop border searches have a precise analogy to a previous, failed government effort to impose surveillance on computing. During the 1990s, the federal government attempted to regulate the spread of effective encryption for communications over the Internet. Federal law made it illegal to export "strong" encryption -- encryption that could not be easily broken. Most notoriously, the federal government proposed the "Clipper Chip." This chip, built into communications devices, would have provided the government with the encryption keys for communications, so that the government could automatically break the encryption once it had a court order. The "Clipper Chip" came to stand for a broader government attempt to get the encryption keys for private use of encryption, a practice known as "key escrow."

The testimony here gives a common-sense history of this technical area of encryption regulation. For purposes of today's hearing, my point is that laptop border searches are the Clipper Chip all over again. The same criticisms that applied a decade ago to the Clipper Chip specifically, and federal encryption policy more broadly, apply to laptop border searches today.

A decade ago, the flawed federal encryption policy alarmed a wide coalition of business, computer security, privacy, human rights, and many other groups. A large and bipartisan movement arose in Congress to object to the administration policy. This coalition confronted federal law enforcement and national security agencies in what came to be known as the "crypto wars." As shown by the witnesses at today's hearing, the same coalition is beginning to emerge with respect to border laptop searches, and for the same reasons.

As a law professor who wrote about encryption and later as a government official, I was personally involved in the encryption debates. I draw on that experience now to underscore the bad policy and ultimate futility of today's policy of laptop border searches.

Summary of the crypto wars. The crypto wars were widely covered in the press, and the history is told in great deal in writings such as Steven Levy's 2002 book Crypto.[4] I will give just enough of that history to indicate the reasons for concluding that border laptop searches are a close analogy.

Encryption roughly means the process of transforming text to make it unreadable (or very difficult to read) for anyone who does not possess the key for reading the text. Throughout history, encryption was the special province of governments, which kept close control over encryption techniques for military and diplomatic advantage. Two changes occurred by the early 1990's, however, that made encryption far more important to individual and commercial users. First, the Internet began its spectacular growth, especially after commercial activity was authorized on the Internet in 1993. Second, a fundamentally new approach to encryption -- called "public key encryption" -- became widely available. This sort of encryption allows effective encryption to occur even among geographically-separate people who have never met before. With public key encryption, you wrap your message in my "public key" that is posted publicly, and you send it to me. I then unwrap the message using my "private key" and the message has thus been transmitted securely.

Users of the Internet, including the first E-Commerce companies, recognized that strong encryption was essential to the growth of the Internet. E-mails and other traffic on the web rely on "message forwarding" -- my message to you is forwarded through multiple servers, operated by unknown and perhaps malicious owners. If we send our messages in plain text, then those intermediate servers can read the content, make copies, and cause untold problems. To take a simple example, it is a really bad idea to send a payment for $1 million in unencrypted form. One of the intermediate server owners could then make copies, try to cash that $1 million before the legitimate recipient can, and perhaps try to cash it multiple times. Similar problems can arise for non-commercial users, such as human rights groups overseas that are using the Internet to blow the whistle on human rights abuses.

The correct technical solution is strong encryption. Using public-key encryption, a user anywhere in the world can securely send a message to a recipient anywhere in the world. Commercial users, human rights groups, and anyone else thus has a straightforward way to avoid the insecurity that otherwise would exist for every message sent through the Internet.

The problem in the 1990s was that national security and law enforcement agencies vehemently objected to the new encryption technology. The National Security Agency (NSA) had the responsibility of intercepting and reading electronic communications outside of the United States. The NSA was deeply concerned that its collection would "go dark" if strong encryption became the norm. Within the U.S., the Federal Bureau of Investigation was concerned that strong encryption would undermine its ability to conduct wiretaps and read computers when seized. At the time, the main legal tool for the government was a set of rules prohibiting the export of most encryption outside of the United States. Although strong encryption was still permitted within the U.S., it was considered export of a dangerous "munition" to send effective encryption software to other countries.

The clash between the opposing views led to a proposed "compromise" in 1993 called the Clipper Chip. Proponents hoped that their approach would allow government surveillance to proceed effectively even as the private sector used encryption widely. Clipper Chip depended on "key escrow" -- the idea that the government could gain access to a database of encryption keys when a proper wiretap order or other legal basis existed. For supporters of Clipper Chip, this approach would maintain the traditional government ability to conduct a wiretap where the court order was in place. Supporters of Clipper Chip argued that the system would be trustworthy because the government would access the database of keys only with proper legal authority.

The reaction to the Clipper Chip was intense opposition from E-Commerce and other businesses, privacy and civil liberties groups, and a phalanx of computer security experts. I believe the computer

security criticisms were especially effective -- the Clipper Chip would mean deploying a known flaw widely in our communications system; the key escrow database was a single point of failure which, once breached, would compromise an enormous array of communications; and the "trust us" model (the idea that we should trust the government with our encryption keys) was not good enough given the U.S. and other governments' weaknesses in computer security.[5]

These technical criticisms of the key escrow were picked up by an increasingly effective political coalition of civil liberties and business groups. A growing chorus of criticism came from the Congress. By 1999, over 250 members of the House of Representatives had signed onto the Security and Freedom Through Encryption ("SAFE") Act, and opposition to the administration in the Senate was led by a bipartisan coalition featuring the unusual pair of John Ashcroft and John Kerry.[6] The proposed legislation would have blocked the key escrow approach, by which government would gain control of encryption keys, and would have opened up exports of strong encryption for E-Commerce and other purposes.

During this period there were intense discussions in the executive branch about how to proceed on encryption policy. Along with many others, I participated in this process, and I know that the computer security vulnerabilities caused by key escrow were intensively discussed. On September 16, 1999 the Clinton Administration announced a major shift in encryption policy, putting the U.S. on a path toward lifting most controls on the export of encryption. In my role as Chief Counselor for Privacy, I had the honor of speaking at the White House event announcing the change in encryption policy:

> I am here to underscore that today's announcement reflects the Clinton Administration's full support for the use of encryption and other new technologies to provide privacy and security to law-abiding citizens in the digital age. The encryption measures announced today properly balance all of the competing interests, including privacy, electronic commerce, and public safety. Encryption itself is a privacy and security enhancing technology. Especially for open networks such as the Internet, encryption is needed to make sure that the intended recipients can read a message, but that hackers and other third parties cannot. Today's announcement will broaden the use of strong mass market encryption for individuals and businesses.[7]

After the 1999 announcement, the use of strong encryption on the Internet and more generally was clearly established. Strong encryption, including for export, has remained legal since that time.

The Analogy Between Laptop Border Searches and the Encryption Policy of the Clipper Chip

The testimony now turns to the eight comparisons between the encryption policies of the 1990s and laptop border searches today:

1. Traditional legal arguments apply badly to new facts about computing
2. Government forces disclosure of encryption keys
3. Severe violation of computer security best practices
4. U.S. policy creates bad precedents that totalitarian and other regimes will follow
5. Severe harm to personal privacy, free speech, and business secrets
6. Disadvantaging the U.S. economy
7. Political coalition of civil liberties groups and business
8. Technical futility of U.S. policy

1. **Traditional legal arguments apply badly to new facts about computing**

In the crypto wars, the government relied on legal tradition -- wiretap orders historically were issued by judges, and such orders enabled the government to listen to the content of phone calls and other communications. Similarly, search warrants were issued upon probable cause, allowing physical access to computers. In the eyes of law enforcement officials, the Clipper Chip and other key escrow measures were needed in order to maintain the status quo. Without key escrow, in their view, wiretap orders and search warrants would often be frustrated by the technique of encryption. For many in government, it thus seemed obvious common sense to maintain the status quo of effective government access to information, once the wiretap order or search warrant had been issued.

Opponents of government regulation responded, effectively in my view, that key escrow was an unprecedented measure that did not recognize the fundamental facts of modern computing. In the physical world, we do not give the keys to our front doors to the government. Key escrow was unprecedented because of its requirement that each person affirmatively hand over the key in advance. In addition, key escrow would enable an unprecedented scale and scope of government surveillance. Key escrow in communications would enable access to the vastly increased flow of information enabled by the Internet, modern computers, and the reduction in the cost of telecommunications. Key escrow access to our physical computers would allow one-stop surveillance of a person's enormously detailed computer files.

Turning to laptop border searches, the government relies once again on a traditional legal argument. The government points out that there is a long history of physical searches when a person crosses the border, so there is nothing new at all about physical searches of laptops and other modern computing devices. Their legal argument roughly says: "Nothing to see here; move along."

As with key escrow, however, there is something to see here. The government's position essentially is that they can make the traveler open a suitcase, so they can make the traveler open a laptop. A modern laptop, however, holds exponentially more material than a physical suitcase. The 80 gigabytes of today' standard laptop could likely hold all the books printed in human history up through sometime well into the 20th century. Not only does the government get access to an unprecedented wealth of material with a laptop border search, but the government now has the ability to copy, store, and analyze that information at its leisure. Government agencies have access to the "Computer Online Forensic Evidence Extractor," a thumb drive designed to quickly extract and copy a complete image of a laptop or other computer.[8] In traditional border searches, travelers carried their suitcases with them once they cleared customs. With laptop border searches, the government can keep everything in the computer in perpetuity. With key escrow, the government position was "trust us" not to look at all the communications it could read. With laptop border searches, the government once again says "trust us" with all the data it can read.

2. **Government forces disclosure of encryption keys**

A central front in the crypto wars was whether users would be required to disclose their "private keys" to the government. As described above, the system of public key encryption was coming into common use as the Internet grew in the late 1980s and early 1990s. With public key encryption, you wrap your message in my "public key" that is posted publicly, and you send it to me. I then unwrap the message using my "private key" and the message has thus been transmitted securely.

For people who did not live through the encryption debates of the 1990s, it is probably hard to imagine how strongly many computer security experts feel about revealing their private keys. A quote from John Perry Barlow, co-founder of the Electronic Frontier Foundation, helps provide insight. Responding to a key escrow proposal, Barlow said: "You can have my encryption algorithm, I thought to myself, when you pry my cold dead fingers from its private key."[9]

For laptop border searches, the government is once again demanding that individuals and businesses turn over their passwords and encryption keys. Travelers are given the "choice" of handing over their keys or else being refused entry into the country. Because disclosure of encryption keys was such an intense flash point in the 1990s, the Customs and Border Patrol policy of demanding encryption keys may well prove far more controversial than its officials have realized.

3. Severe violation of computer security best practices

In the encryption debates, computer security experts played a central role in explaining why key escrow proposals would undermine secure communications for all applications on the Internet. In a world where people were routinely communicating across borders, it was vital to use strong encryption to conduct communications and transactions in a secure way.

A decade later, computer security has become an even greater priority in light of our experience with problems such as spam, spyware, viruses, and other sorts of malware. Computer hacking has evolved from its prankster roots into an organized business, featuring large "bot farms" that allow organized crime to launch large and effective attacks through computers they have infected. Federal agencies and major corporations have been repeatedly hacked, amidst growing reports of cyberattacks from overseas, some of them likely with government support. There have been growing reports of "root kits," where outside software gives hackers access to the "root" or fundamental control of the computer.

Data breaches have been a top story in the area of computer security. Most states have passed laws requiring notices to consumers about data breaches, and the Privacy Rights Clearinghouse has documented over 226 million data records of U.S. residents that have been exposed due to security breaches since 2005.[10]

In response to these daunting challenges, responsible corporations and individuals have instituted much stricter computer security. Users outside of the company are generally strictly forbidden from gaining access to the computer and its files. Controls are installed to make it harder to copy data through thumb drives and other external devices. Many corporations have instituted training and other procedures to reinforce the importance of not exposing the company's data to outsiders.

In response to the problem of data breaches, corporate America is rapidly shifting to a norm of encrypting the hard drives of laptops and other computers. The reason is that data breach laws have an exemption from notice where the data is encrypted. Once the hard drive is encrypted, the company saves the expense and problems of notice even if the laptop is lost. Another reason for the shift to hard-drive encryption is that Vista and other recent software makes it more user-friendly to routinely encrypt files in a laptop.

In this environment of heightened computer security, laptop searches at the border are a direct and flagrant violation of industry best practices. Private encryption keys are not supposed to be disclosed, but CPB demands those keys. Thumb drives and other devices for copying large amounts of data are routinely disabled, yet CPB mirrors the entire hard drive full of corporate or individual data. Turning over the computer to the government, with passwords and encryption disabled, also exposes the computer to the risk of root kits and other malware -- the computer cannot be treated as a trusted platform under industry best practice once it was been opened wide to a third party such as the government.

4. U.S. policy creates bad precedents that totalitarian and other regimes will follow

If the United States adopts a policy, then it is generally much harder for the U.S. to object if other countries adopt a similar policy. This problem arose with the key escrow approach to encryption. Even if you trust handing your encryption keys to the U.S., would you feel the same way handing the keys to all your communications to a totalitarian regime? A common theme in the encryption debates was that numerous countries would want to follow the U.S. lead and gain access to encryption keys, with many negative effects on commerce, free speech, theft of trade secrets, and so on.

The same applies to laptop border searches today. I explained just now why divulging passwords and encryption keys at the border violates modern security practices. Perhaps many of us would trust the Customs and Border Patrol itself, especially if careful procedures and audits were developed to protect against the risk of breach or mis-use of data. The problem would remain, however, that totalitarian and other countries would quite possibly imitate the U.S. border policy. For Senators and their staffs, would you want the entire contents of your laptops revealed to foreign governments? If Senators and their staffs are subject to such searches in the future, then the ability of the U.S. government to object will be at low ebb. By contrast, thoughtful policies for U.S. border searches, including being based on reasonable suspicion or probable cause, would provide a much more effective basis for the U.S. to object to overly intrusive border searches by other countries.

5. Severe harm to personal privacy, free speech, and business secrets

For reasons already described, the key escrow approach to encryption threatened severe harm to personal privacy, free speech, and business secrets. Privacy was threatened because the government kept the keys that enabled it to listen to any communication. Free speech was chilled because of the concern that the U.S. or any other government would be listening. Business secrets were at risk, and the security of business transactions was threatened, because the Internet was being based on insecure technology rather than strong encryption.

The same applies to laptop searches at the border. The Electronic Frontier Foundation and the Association of Corporate Travel Executives, on their websites, describe many of the scenarios that make such searches especially intrusive. For personal privacy, an individual's laptop may well contain diaries, love letters, a lifetime of saved email, private photos, passwords, financial and medical records, and evidence of almost any other intimate part of life. The text of the Fourth Amendment protects "persons, houses, *papers, and effects*." (emphasis supplied) This constitutional text highlights the Framers deep concerns about personal papers and related documents. There is a long history in the Supreme Court of granting especially strong protection to diaries and similarly personal papers.[11] Even if such "papers and effects" do not gain absolute protection under current Fourth Amendment doctrine,

this long history of concern should inform our government's policy toward searching through an individual's lifetime trove of personal papers.

Intrusive laptop searches by the U.S. and other governments would similarly chill free speech. One vivid example is a human rights activist entering or leaving China, perhaps on a religious or other mission that is controversial in that country. More generally, laptop searches make a trip across the border a potentially scary moment when legitimate First Amendment speech can be placed in a government database, with no known limits on how the computer files are saved and used. For example, someone in the opposite political party from the President could worry that campaign plans and other political activities would be copied and saved by the Department of Homeland Security. The government may say that they would not do such things, but the lack of legal safeguards once again means that we must simply trust the government not to mis-use its power.

The harm to business secrets from laptop searches is similarly substantial. The harm begins with the security violation of revealing passwords and private encryption keys; if the passwords or keys are used in any other settings in the company, then changes must be made in all of those other settings or else the system is exposed to additional intrusion. Others have catalogued other costs and problems that business confronts: exposure of trade secrets; compromise of the attorney-client privilege for material viewed by third parties; journalists' notes that would be protected by shield laws; and others. At the very least, businesspeople face the risk that their business will be interrupted by government taking of their laptop or PDA, even if "only" for a week or two. In the face of that risk, prudent businesses will increasingly have to resort to costly supplementary measures to ensure that important business information will make it past the border each and every time. Laptop border searches thus impose a new and costly tax on crossing the border.

6. Disadvantaging the U.S. economy

In the 1990s, it became increasingly apparent over time that U.S. encryption policy was harming the U.S. economy and advantaging competitors in other countries. The encryption limits specifically applied to exports from the U.S. to other countries. U.S. software and hardware companies were thus prevented from selling strong encryption to global markets. Over time, competitors in other countries, including Russia, started to sell high-quality encryption products and began to gain significant market share. A disadvantage of U.S. encryption policy was thus that sales that would have gone to U.S. companies were shifting instead to foreign competitors.

The same critique applies to laptop searches at the U.S. border. Foreign tourists will not like the idea of having their laptop inspected at the border, and may decide to visit elsewhere. International conferences and conventions will choose to locate elsewhere. Business travelers, at the margin, will decide to use teleconferences or otherwise skip the annoyance and risk of coming to the U.S. for a meeting. Laptop searches are one part of a broader issue about the extent to which the United States seeks to be open for business and open for tourism. Laptop searches send the signal that crossing the U.S. border may well be an unpleasant and intrusive experience. If laptop searches were vital to the fight against terrorism, then we might craft procedures to do them while minimizing the intrusion. The available cases, however, are not about terrorism-related investigations. For this reason, it may be useful for the Committee to ask the U.S. Department of Commerce to estimate the effects on the U.S. economy of laptop border searches.

7. Political coalition of civil liberties groups and business

The crypto wars featured an effective coalition of civil liberties groups and the business community. Civil liberties groups highlighted the negative effects of administration policy on privacy, security, free speech, human rights efforts, and other causes. The business community emphasized how encryption policy was negatively affecting growth of the Internet, putting trade secrets at risk, and disadvantaging American business at the expense of competitors overseas.

The hearing today shows that this same coalition is developing on the issue of laptop border searches. Testimony today comes from civil liberties groups such as the Electronic Frontier Foundation and Muslim Advocates, and a diverse and impressive set of civil liberties organizations have signed a letter objecting to current practices.[12] Also testifying today, as a sign of business concern, is the Association for Corporate Travel Executives. I can add, from my personal experience, that the current practices generate outrage and incredulity from a range of business executives and corporate security officers with whom I have discussed the issue. For instance, after I was asked to testify at this hearing, I raised the issue with a group of business people for global companies. They had been growing increasingly aware of the issue in the past year, and were contemplating a variety of expensive and inconvenient options for their companies, including prohibiting travel with normal laptops and instead issuing separate "travel computers" that would be thoroughly scrubbed before each border crossing.

Because the *Arnold* decision upholds intrusive laptop border searches, with no requirement of government suspicion, I believe the concern from both a business and civil liberties perspective will likely grow quickly. In the wake of the *Arnold* decision, there has already been increased discussion in technical circles on the web about what to do in the face of intrusive laptop searches. I hope this hearing will help avert the need for the large-scale and lengthy political mobilization that was required to reverse the worst aspects of encryption policy in the 1990s.

8. Technical futility of U.S. policy

One of the final arguments against U.S. encryption policy in the 1990s was that it was ultimately futile as a technical matter. The U.S. rules said it was illegal to export strong encryption, but it was impossible at a practical level to prevent transfer of encryption software from the U.S. to other countries, whether over the Internet or through the mail or physical delivery. In addition, over time, buyers outside of the United States were increasingly able to buy strong encryption from non-U.S. suppliers. The strict U.S. rules were ultimately repealed in part due to a recognition that they were simply not succeeding at preventing the spread of encryption.

Similarly, laptop searches will not succeed at a technical level at preventing data from entering or leaving the U.S. Computer security researcher Chris Soghoian in May posted a story called "Keep Your Data Safe at the Border."[13] Soghoian presents an eight-point checklist for how to get your data legally across the border without being searched. The primary trick is to send encrypted files to yourself once you get to your destination country.

The Soghoian article shows the futility yet burden imposed by laptop searches at the border. Any terrorist who is even moderately well informed can learn how to send the crucial files legally and safely across the border. In addition, a terrorist who is willing to lie to the customs agent (certainly a possibility worth considering) can use TrueCrypt or other software that does the following trick -- it allows you to encrypt a secret cache of data inside your encrypted hard drive. Then, when an investigator forces you to open your encrypted files, the secret cache remains invisible to the

investigator. This TrueCrypt approach requires lying to the custom agent about whether you have opened up all of your files, but it is a technical measure already available with widely-available software.

Although these approaches show the inability of laptop border searches to catch moderately smart criminals or terrorists, the approaches are costly and burdensome. Companies, civil society groups, and individuals who do not want their data read are forced to go through fairly complex contortions to prevent access by the government at the border. As with the crypto wars in the 1990s, a system that can be evaded by competent criminals but imposes large costs on honest citizens should be avoided.

In conclusion, I thank the Committee for the opportunity to address these important issues, and I would be glad to answer any questions.

---

[1] The briefs and other materials in *U.S. v. Arnold* are available at http://www.eff.org/cases/us-v-arnold.
[2] Katherine Strandburg, "Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance," 49 Boston College L. Rev. No. 741 (2008), available at http://ssrn.com/abstract=1136624.
[3] Daniel J. Solove, "The First Amendment as Criminal Procedure," 82 N.Y.U. L. Rev. 112 (2007), available at http://ssrn.com/abstract=924900.
[4] Steven Levy, Crypto: How the Code Rebels Beat the Government: Saving Privacy in the Digital Age (2002)
[5] The Center for Democracy and Technology assembled 11 of the leading computer security experts to write a report called "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption," (1998), available at http://www.cdt.org/crypto/risks98/.
[6] See "Summary of Encryption Bills in the 106th Congress," available at http://www.techlawjournal.com/cong106/encrypt/Default.htm.
[7] Transcript of Special White House Briefing on Encryption Technology, Sept. 16, 1999, available at http://seclists.org/politech/1999/Sep/0023.html.
[8] Benjamin J. Romano, "Microsoft device helps police pluck evidence from cyberscene of crime," Seattle Times, April 28, 2008, available at http://seattletimes.nwsource.com/html/microsoft/2004379751_msftlaw29.html.
[9] John Perry Barlow, "Decrypting the Puzzle Palace," (1992), available at http://www.matarese.com/matarese-files/5969/decryptingpuzzle-palace-john-perry-barlow-july-1992/index.html.
[10] Privacy Rights Clearinghouse, "A Chronology of Data Breaches," available at http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[11] The leading Supreme Court case is U.S. v. Boyd, 116 U.S. 616 (1886). See Peter P. Swire, "*Katz* is Dead; Long Live *Katz*," 102 Mich. L. Rev. 904 (2004) (discussing the history).
[12] The letter, with signatories, appears at http://www.muslimadvocates.org/docs/Coalition_sign_on_letter_re_invasive_border_interrogations_--_SJC.pdf.
[13] Chris Soghoian, "Keep Your Data Safe at the Border," CNet, May 5, 2008, available at http://news.cnet.com/8301-13739_3-9935170-46.html.

Statement of Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation
Before the U.S. Senate Committee on the Judiciary Subcommittee on the Constitution
"Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel"
June 25, 2008

Mr. Chairman and Members of the Judiciary Committee Subcommittee on the Constitution, the Electronic Frontier Foundation ("EFF") is pleased to have this opportunity to discuss with you an issue of growing importance to Americans' privacy – unchecked government power to search or seize American travelers' portable electronic devices at the border, whether laptop computers, iPhones, BlackBerries or digital cameras.

EFF is a non-profit, member-supported public interest organization dedicated to protecting privacy and free speech in the digital age – an age in which ordinary Americans, from tourists to business travelers, use portable electronic devices to store personal thoughts, communications with family, friends and professional colleagues, Internet searches, and banking and medical information.

What is your deepest secret? Do you have any embarrassing health conditions? Have you ever had a family crisis? What are the details of your finances? Do you have trade secrets or confidential information related to your work? The answers to questions like these are often contained on laptops and similar devices. Any reasonable person would say that Americans have a legitimate expectation of privacy in such information. Indeed, in his April appearance before the full Committee, Department of Homeland Security ("DHS") Secretary Chertoff agreed that "there are absolutely privacy concerns" in searching laptop computers at the border.

We also use electronic devices to research, communicate, publish, and perhaps most important, think. A blogger's laptop undoubtedly reflects not only private thoughts but also drafts of works in progress, contact information for sources, and confidential records. Laptops, cell phones, BlackBerries, iPhones and other personal devices are used not only to store information but to communicate with others via email, instant messenger services, blogs, chat rooms, and bulletin boards, and to read information

from the Internet, a new and powerful medium of expression that covers a range of topics "as diverse as human thought." *Reno v. ACLU*, 521 U.S. 844, 852 (1997); *id.* at 863 (the Internet "is the most participatory form of mass speech yet developed, entitled to the highest protection from governmental intrusion.") (internal citations omitted).

This protection is not limited to the contents of a person's writings or communications; it extends to his or her identity and the identity of his or her correspondents. In the modern context, it includes knowledge about a person's interests, the websites he or she reads, and the electronic files that he or she downloads. "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation -- and their ideas from suppression -- at the hand of an intolerant society." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (citation omitted). Thus, both freedom of expression and freedom of association are at stake as well, because arbitrary government access to these devices will chill speech as people question whether what they say and think (and to whom) is proper.

In short, these devices are virtual extensions of the person; "they are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more." Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005) ("Kerr"). We greatly value the privacy of our laptops and similar devices precisely because they embody so much of our lives.

As part of our public-interest mission, EFF is currently engaged in litigation to protect our precious rights to privacy and freedom of speech in this area. Along with the Asian Law Caucus ("ALC"), we are fighting a Freedom of Information Act lawsuit against U.S. Customs and Border Protection ("CBP") for records about CBP's policies and practices regarding interviews and searches at U.S. ports of entry. Over the past year, ALC and EFF have received numerous inquiries from U.S. citizens and residents in northern California regarding CBP's actions, including concerns about the detailed examination by CBP officers of reading material and sensitive personal information, including books, appointment calendars, notebooks, laptop computer files, cell phone directories, and other materials. This case is currently pending in the U.S. District Court in the Northern District of California.

EFF is also amicus curiae, along with the Association of Corporate Travel Executives, in *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008), *petition for rehearing en banc pending*, currently before the Ninth Circuit U.S. Court of Appeals. That case upholds the power of government border agents to search and seize data and devices without any showing of suspicion whatsoever.

CBP's use of the Fourth Amendment border search doctrine poses a significant threat to American travelers' privacy. The threat comes not only from arbitrary searches, but also from the increased storage capacity of modern devices and from searches enabled by forensic technology, which means private information may be more thoroughly and efficiently searched than ever before – inexpensive tools now allow border agents to easily copy all data from laptops and other portable devices.

Ideally, the courts would interpret the border search doctrine in a reasonable way. The courts, however, are not the sole guarantors of our constitutional rights. As Senator Leahy noted when Congress enacted the Electronic Communications Privacy Act, "the law must advance with the technology to ensure the continued vitality of the fourth amendment." S. REP. NO. 99-541 at 5 (1986).

That same issue is posed here. The border search doctrine has long authorized extensive, highly discretionary searches. In the past, however, border searches were unlikely to invade every domain of an individual's life. A traveler might carry extensive paper files across the border, but such cases have been rare; with computers, the problem is common, not exceptional. Technology now puts massive amounts of personal and proprietary communications and information within border officials' grasp: as a former head of the Justice Department's computer crime unit put it,

> While most people do not travel internationally with a copy of every chat they have ever had, or every Facebook friend's picture in their Samsonite, or every picture they have of their boyfriends or girlfriends, they have exactly this information on their laptops. They have their checkbook information, passwords, financial records, medical records, correspondence,

records of books purchased, Web sites reviewed, and more. In short, communicative and expressive materials.[1]

I will begin with a brief description of the border search doctrine.[2] Then I will explain why EFF believes that searches of laptops and other portable electronic devices should be governed by at least a "reasonable suspicion" standard. Finally, I will conclude with some thoughts about what Congress can do to address this problem.

The Fourth Amendment governs searches and seizures conducted by government officials. Under the border search doctrine, however, government officials at the nation's borders may conduct "routine" searches of individuals and their personal effects without suspicion, judicial approval or a warrant. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

Nevertheless, the Fourth Amendment does apply at the border. As Chief Justice Rehnquist wrote, "Balanced against the sovereign's interests at the border are the Fourth Amendment rights of respondent. . . . [who] was entitled to be free from unreasonable search and seizure." *Id.* at 539.

Put another way, even border searches must be *reasonable*.

While a routine border search is reasonable by definition, not all border searches are routine. Many courts have held strip searches, body cavity searches, and involuntary x-ray searches to be non-routine, requiring reasonable suspicion. There is no bright-line rule here, but the Supreme Court has said that non-routine searches are partly defined by their invasion of a person's dignity and privacy interests. *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004) ("the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person – dignity and privacy interests of the person being searched – simply do not carry over to vehicles").

---

[1] Mark D. Rasch, *On the Border*, http://www.securityfocus.com/columnists/469 (March 20, 2008).

[2] A summary of the law is contained in Congressional Research Service, *Border Searches of Laptops and Other Electronic Storage Devices*, RL34404 (March 5, 2008).

These principles – the dignity and privacy interests of the person being searched – establish the need to treat border searches of laptops and similar devices as non-routine. We do not challenge the proposition that physical searches of devices for drugs, explosives, and so on, are routine searches. But as the district court in *United States v. Arnold* wrote:

> A laptop and its storage devices have the potential to contain vast amounts of information. People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records. Attorneys' computers may contain confidential client information. Reporters' computers may contain information about confidential sources or story leads. Inventors' and corporate executives' computers may contain trade secrets.

United States v. Arnold, 454 F.Supp.2d 999, 1003-04 (C.D. Cal. 2006).

This approach is fully consistent with the Fourth Amendment, which protects the privacy of persons as thinking, feeling beings: as Justice Brandeis's famous dissent in *Olmstead* recognized, "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect." *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *rev'd*, *United States v. Katz*, 389 U.S. 347 (1967). This aspect of privacy, which the Supreme Court eventually recognized in *Katz*, is at stake in laptop border searches.

We believe that any kind of information search of these devices should be viewed as a non-routine search requiring reasonable suspicion. We have already noted that the nature or quality of the information on laptops is highly personal. But the quantity of information stored on a laptop is also far greater than could possibly be carried in a briefcase. "Computer hard drives sold in 2005 generally have storage capacities of about eighty gigabytes, roughly equivalent to forty million pages of text — about the amount of information contained in the books on one floor of a typical academic library. These figures will soon be outdated, as computer storage capacities tend to double about every two years. . . . While computers are compact at a physical level, every computer is akin to a vast warehouse of information." Kerr, at 541-542 (footnotes omitted). Perhaps neither quantity nor quality alone would be enough, but the combination

clearly distinguishes laptops and similar devices from non-informational property like vehicles.

Furthermore, laptops and other devices contain data almost never found in paper documents. "Common word processing programs such as WordPerfect and Microsoft Word generate temporary files that permit analysts to reconstruct the development of a file. Word processing documents can also store data about who created the file, as well as the history of the file." Kerr, at 543 (footnotes omitted). "Similarly, browsers used to surf the World Wide Web can store a great deal of detailed information about the user's interests, habits, identity, and online whereabouts, often unbeknownst to the user. . . . Some of this information may be very specific; for example, the address produced by an Internet search engine query generally includes the actual search terms the user entered." *Ibid.* (footnotes omitted). Indeed, Web browsers often retain not only the Internet addresses of sites one has visited, but actual information, both text and images, accessed during the visit, even when the user had no intent to copy such information.

Thus, where a laptop or similar device is concerned, a person's dignity and privacy interests are squarely at issue. Prof. Kerr has observed that "[a]s our computers perform more functions and preserve more data, we may eventually approach a world in which a considerable chunk of our lives is recorded and stored in perpetuity in our computers. These details may end up stored inside our machines in a way that can be reconstructed later by a forensic analyst with remarkable accuracy." Kerr, at 569. As a result, "computer searches tend to be unusually invasive." *Ibid.*

It should come as no surprise, then, that a major law firm like Arnold and Porter recently (Feb. 2008) warned its clients about the risks of laptop border searches: "Electronic storage devices contain vast amounts of information, and because that information frequently can be sensitive or personal or even privileged, reviewing the contents of an electronic storage device seems less like a 'routine' border search than riffling through a traveler's clothes."[3]

---

[3]http://www.arnoldporter.com/public_document.cfm?u=WorkingOnTheFlightHowInternationalTravelCanResultInGovernmentOfficialsExaminingYourElectronicData&id=10376&key=22G0.

The problem runs deeper, however. Because of the quantity and nature of information stored on laptops and similar devices, the border search doctrine creates a scope problem. Limits on the scope of a search are inherent in the very concept of reasonableness that is the touchstone of Fourth Amendment law, even at the border. Border searches of laptops are, in effect, forbidden general, indiscriminate searches.[4]

The more apt precedent here is *Katz v. United States*, 389 U.S. 347 (1967), in which the Supreme Court clearly established that the Fourth Amendment protects private telephone calls made from phone booths. *Katz* overruled the 1928 *Olmstead* decision, which had held that police wiretaps did not violate the Fourth Amendment when the wiretaps were installed in publicly accessible locations because there was "no entry of the houses [or] offices of the defendants." *Olmstead*, 277 U.S. at 464.

Under *Katz*, privacy protects persons, not places, and extends to private communications. *Katz* also made clear that constitutional protections must evolve with modern technology and social practices. In rejecting *Olmstead*'s "trespass" approach to the Fourth Amendment, the Supreme Court explained: "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Katz*, 389 U.S. at 352.

The same values and logic apply here. The *Arnold* panel's reflexive embrace of the "container" analogy and casual rejection of privacy and speech interests in the contents of one's laptop is the modern equivalent of the *Olmstead* Court's mechanical application of the "trespass" approach to wiretapping. Laptops, iPhones and BlackBerries are central to private communication today. Under *Katz* and its progeny, border searches of laptop computers cannot be routine; to do so would ignore their "vital role" in private communication.

Privacy and free speech are related in yet another way. The Supreme Court has long been vigilant about the potential for overreaching governmental power to chill speech. "It is characteristic of the freedoms of

[4] Searches must be limited in scope because "[g]eneral warrants . . . are prohibited by the Fourth Amendment." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). The concern is "not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." *Id.* (internal quotation marks and citation omitted).

expression in general that they are vulnerable to gravely damaging yet barely visible encroachments." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963). The danger of unauthorized official surveillance parallels the danger of official censorship, which derives "not merely [from] the sporadic abuse of power by the censor but the pervasive threat inherent in its very existence." *Thornhill v. Alabama*, 310 U.S. 88, 97 (1940).

This concern links the First and Fourth Amendments. The Framers adopted the Bill of Rights "against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961). Surveillance of private communications therefore poses a grave danger to free speech, because "fear of unauthorized official eavesdropping" may "deter vigorous citizen dissent and discussion of Government action in private conversation." *United States v. U.S. Dist. Ct.*, 407 U.S. 297, 314 (1972). Accordingly, the Fourth Amendment must be applied with "scrupulous exactitude" when First Amendment material is at stake. *Stanford v. Texas*, 379 U.S. 476, 485 (1965).

Thus, in *Heidy v. U.S. Customs Service*, 681 F. Supp. 1445 (C.D. Cal. 1988), the district court explained that "[b]order search cases relaxing fourth amendment standards solely for the purpose of facilitating detection of physical objects sought to be imported unlawfully . . . are inapposite to this [informational] case." *Id.* at 1450 (footnote omitted). The court further stated that "limited reading or perusal of writing that appears on objects sought to be imported inevitably may be required for the purpose of identifying the objects themselves," but "a reading for the purpose of revealing the intellectual content of the writing requires encroachment upon first amendment protections far beyond the mere search and seizure of materials." *Id.*

Requiring reasonable suspicion is highly unlikely to impede border agents in their effort to prevent contraband from crossing the border, because it is not a high standard. *See Montoya de Hernandez*, 473 U.S. at 533 (describing how international traveler was nervous, did not know where she was going to stay, had packed inappropriate items for a vacation in Miami, and had limited cash); *United States v. Ickes*, 393 F.3d 501, 502-03 (4th Cir. 2005) (describing how traveler was acting suspicious, brought superfluous items with him on his alleged vacation, and officers discovered an outstanding warrant during a routine search).

In virtually all laptop border search cases, courts have found reasonable suspicion. As one commentator put it: "The threshold for reasonable suspicion at the border is so low, in fact, that the only circumstance that would likely not meet this standard is a complete lack of suspicion, or a random search." Christine Colletta, Note, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 BOSTON COLL. L. REV. 971, 983 (2007) (footnote omitted).

Thus far, we have only considered searches of laptops and other devices. But border agents often go much further, such as by copying data and seizing devices. In our view, these actions are seizures, not border searches, and should be subject to more stringent standards.

When the government copies information stored on electronic devices, it seizes that information, as distinct from searching the device. Seizure is traditionally defined as that which "meaningfully interfere[s]" with a "possessory interest." *Arizona v. Hicks*, 480 U.S. 321, 324 (1987) (*quoting Maryland v. Macon*, 472 U.S. 463, 469 (1985)); *see* Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, *67 ("When the police use a packet sniffer, use a hard-drive imager, or keep data subject to withdrawn consent, a seizure has occurred. The owner of the information has lost the ability to delete, modify, secrete, or contextualize a copy of the information, even though he may have retained his own copy. No less than when the police commandeer an automobile or grab a box of records, the owner of the intangible property has lost dominion and control over his property."). Thus, government copying infringes the traveler's possessory interest in his or her information, above and beyond the privacy interest infringed by visual inspection. The same is true for device seizures.

It is unclear what standard DHS uses or believes is lawful. In his April appearance before the full Judiciary Committee, Secretary Chertoff stated that reasonable suspicion was sufficient to justify copying data; later, however, he said that "the standard is probable cause" when DHS copies or otherwise retains the contents of a person's laptop. Clarity is needed here.

My final substantive point is that technology has exacerbated the problem we face here in more than one way. We value technology because of its convenience and its productivity. Ordinary Americans are enjoying

the fruits of our innovation by using portable devices like laptops and iPhones. But technology is also making it far easier to search those devices.

The combination of technology and the border search doctrine must not be allowed to swallow up the Fourth Amendment rights of international travelers. While at least one court found the possibility that "any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer 'hard drive'" to be "far-fetched," *United States v. Ickes*, 393 F.3d 501, 506-507 (4th Cir. 2005); *id.* at 507 ("Customs agents have neither the time nor the resources to search the contents of every computer."), it is not.

First, customs officials will improve their ability to search laptops, making it increasingly likely that more border searches of computers will be practical in the future than today. If border agents can legally search *any* device at the border, then they can legally search *every* device at the border – *any* really means *every*. Without a legal standard, investigative resources are the only limit on searching ordinary Americans' devices, and technology is quickly removing that constraint.

• In February, Microsoft announced a device named COFEE, which stands for Computer Online Forensic Evidence Extractor. The COFEE is a USB thumb drive that "contains 150 commands that can dramatically cut the time it takes to gather digital evidence. . . . It can decrypt passwords and analyze a computer's Internet activity, as well as data stored in the computer. . . . the investigator can scan for evidence on site."[5]

• In May, the "CSI Stick" (Cell Seizure Investigator Stick) was announced. The CSI Stick is a thumb drive size device that forensically acquires data from cell phones. It can capture all the data off the phone, or just grab SMS messages, phonebooks and call logs, or multimedia messages.[6]

---

[5] Benjamin Romano, *Microsoft device helps police pluck evidence from cyberscene of crime* (April 29, 2008)
http://seattletimes.nwsource.com/html/microsoft/2004379751_msftlaw29.html

[6] *CSI Stick: A thumb drive for searching cellphones* (May 14, 2008)
http://www.fourthamendment.com/blog/index.php?blog=1&title=csi_stick_a_thumb_drive_for_searching_ce&more=1&c=1&tb=1&pb=1

CBP may already be using these kinds of devices, and my point is not that they should not – there may be cases in which such use is appropriate. But we cannot ignore the obvious fact that their use greatly expands agents' practical ability to search for personal and business information unrelated to the purpose of the border search doctrine. "The Fourth Amendment imposes limits on search-and-seizure powers in order to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals." *United States v. Martinez-Fuerte*, 428 U.S. 543, 554 (1976).

Second, even if not every computer is searched, there would still be reason for concern about the effects of enhanced search capacities. Whenever law enforcement exercises unchecked power over its citizens, there is great risk that the government will abuse that power. EFF is thus concerned that the government may access a traveler's computer using the border search doctrine as a pretext to access travelers' data for reasons unrelated to enforcing customs laws – i.e., that the government may use the border search doctrine as an end-run around the constitutional warrant requirement that exists for domestic searches.[7]

If the government lacks probable cause to search a traveler's laptop computer inside the United States, the government may exploit the border search doctrine by waiting until the person travels internationally. Given the frequency of international travel in the modern era, and given the commonness of laptop computers and similar electronic devices, it is reasonable to fear that some law enforcement officers would exploit such a loophole, if the courts permit.

Indeed, there are strong indications that the government is targeting persons based on pre-existing suspicions about their domestic activities, unrelated to concerns about contraband or other concerns identified by Customs agents at the border. An L.A. Times editorial reported that the government claimed that customs officials do not randomly search travelers'

[7] Border searches "made solely in the enforcement of Customs laws" must be distinguished "from other official searches made in connection with general law enforcement." *Alexander v. United States*, 362 F.2d 379, 381 (9th Cir. 1966), *cert. denied*, 385 U.S. 977 (1966) ("Congress has in effect declared that a search which would be 'unreasonable' within the meaning of the Fourth Amendment, if conducted by police officers in the ordinary case, would be a reasonable search if conducted by Customs officials in lawful pursuit of unlawful imports.").

laptops, instead targeting on the basis of a background check or travel plans. Editorial, *Looking into laptops*, L.A. Times, Nov. 11, 2006, at 20. Secretary Chertoff, moreover, told the full Committee in April that being subject to secondary screening "by definition" constitutes "reasonable suspicion."[8]

For all of these reasons, EFF recommends that Congress consider protecting all devices that are highly likely to contain email and other stored communications and communications records. Congress should also clarify that the seizure of data and devices is more than a border search and requires probable cause. We emphasize that in this digital age, the use of basic technical precautions – like password-protecting one's device or encrypting one's data – is reasonable and cannot be the basis for any kind of suspicion.

Secretary Chertoff told the full Judiciary Committee in April that "as a matter of practice," DHS searches the contents of laptops or cell phones "only . . . where there's a reasonable suspicion," and that he believed DHS uses a "probable cause" standard before seizing a searched device or retaining copies of its contents. If so, then there is no reason not to codify these standards into law.

Finally, Congress should establish an administrative oversight regime for laptop border searches and seizures of data and devices that would allow for meaningful oversight by the public, Congress and the courts.[9] The reasonableness of a border search generally depends on legal constraints on

---

[8] In one case a laptop border search was triggered by a computer database alert. *See United States v. Furukawa*, 2006 WL 3330726 at *3 (D. Minn.) (defendant was "referred from passport screening to 'baggage control secondary' based upon a computer screen alert indicating that he may have purchased access to a Internet site that contained child pornography"). *Furukawa* does not provide any further details about the "alert" or the source of the suspicion about defendant, who was eventually acquitted at trial. http://cyb3rcrim3.blogspot.com/2007/05/acquitted.html, *quoting* Dan Browning, *N.Y. Man Cleared of Child-Pornography Charge*, StarTribune.com (May 14, 2007).

[9] The Supreme Court has explained that "bypassing a neutral determination of the scope of a search leaves individuals secure from Fourth Amendment violations only in the discretion of the police." *Katz*, 389 U.S. at 358-359 (internal quotation and citation omitted); *cf. Andresen*, 427 U.S. at 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are . . . among those papers authorized to be seized. Similar dangers . . . are present in executing a warrant for the 'seizure' of telephone conversations. *In both kinds of searches, responsible officials . . . must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.*") (emphasis added).

official discretion.[10] But we are unaware of any public accountability mechanism or carefully drawn policy designed to protect privacy or First Amendment rights for border searches or data and device seizures of travelers' computers. Such a mechanism should be implemented and should include a thorough investigation of DHS's current policies and practices regarding border searches of electronic devices by Congress, the Government Accountability Office, or the DHS Office of Inspector General.

On behalf of EFF, thank you again for the opportunity to present our views.

[10] *Cf. Flores-Montano*, 541 U.S. at 159 (Breyer, J., concurring) ("Customs keeps track of the border searches its agents conduct, including the reasons for the searches. This administrative process should help minimize concerns that gas tank searches might be undertaken in an abusive manner.") (internal citation omitted).

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
ICE Policy System

DISTRIBUTION:	**ICE**
DIRECTIVE NO.:	**7-6.0**
ISSUE DATE:	**July 16, 2008**
EFFECTIVE DATE:	**July 16, 2008**
REVIEW DATE:	**July 16, 2011**
SUPERSEDES:	**See Section 3 Below.**

DIRECTIVE TITLE: BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC MEDIA

1. **PURPOSE and SCOPE.** This Directive sets forth the legal guidelines and establishes policy and procedures within ICE for border search authority to search, review, retain, and share certain documents and electronic media possessed by individuals during investigative operations at the border, the functional equivalent of the border, and the extended border. This Directive applies to all ICE personnel who meet the definition of "customs officer" under 19 U.S.C. § 1401(i) ("ICE Special Agents"), other domestic or foreign law enforcement officers cross designated by ICE as customs officers, and persons whose assistance ICE demands under 19 U.S.C. § 507 (collectively, "ICE personnel"). This Directive applies to searches of documents and electronic media of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise. Each operational office will maintain appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this policy.

   This Directive applies to border search authority only. Nothing in this Directive limits the authority of ICE personnel to act pursuant to other authorities such as a warrant, search incident to arrest, or a routine inspection of an applicant for admission.

2. **AUTHORITIES/REFERENCES.**

2.1 19 U.S.C. § 482, Search of vehicles and persons.

2.2 19 U.S.C. § 507, Assistance for Officers.

2.3 19 U.S.C. § 1401(i), Customs Officers.

2.4 19 U.S.C. § 1461, Inspection of merchandise and baggage.

2.5 19 U.S.C. § 1467, Special inspection, examination, and search.

2.6 19 U.S.C. § 1496, Examination of baggage.

2.7 19 U.S.C. § 1499, Examination of merchandise.

2.8 19 U.S.C. § 1581, Boarding vessels.

2.9 19 U.S.C. § 1582, Search of persons and baggage; regulations.

2.10 19 U.S.C. § 1583, Examination of outbound mail.

2.11 19 U.S.C. § 1595, Searches and seizures.

2.12 19 C.F.R. Part 145, Mail Importations.

2.13 19 C.F.R. Part 162, Inspection, Search, and Seizure.

2.14 8 U.S.C. § 1225, Inspection by immigration officers; expedited removal of inadmissible arriving aliens; referral for hearing.

2.15 8 U.S.C. § 1357, Powers of immigration officers and employees.

2.16 8 C.F.R. § 236.1(e), Privilege of Communication.

2.17 31 U.S.C. § 5317, Search authority for compliance with Currency and Monetary Instruments Reporting Act.

3. **SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES.** Customs Directive 3340-006A, entitled "Procedures for Examining Documents and Papers," dated February 4, 2000, and all other directives, memoranda, bulletins, manuals, handbooks, and other guidelines and procedures relating to this subject and issued by the former U.S. Customs Service or the former U.S. Immigration and Naturalization Service no longer apply to ICE. All other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded, with the exception of the March 5, 2007, OI guidance entitled "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry."

4. **BACKGROUND.** ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, ICE Special Agents may review documents, books, pamphlets, and other printed material, as well as computers, disks, hard drives, and other electronic or digital storage devices. These searches are part of ICE's long-standing practice and are essential to uncovering vital law enforcement information. For example, searches of documents and electronic media are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography, illegal monetary instruments, and information in violation of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

5. **DEFINITIONS.**

5.1 **Assistance.** The use of third party analytic resources, outside of ICE, such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in documents and electronic media or in determining the meaning, context, or value of information contained therein.

5.2 **Documents.** All papers and other written documentation including, but not limited to, those relating to the alien's identity and/or admissibility (e.g., passports, visas, credit cards, licenses, social security cards, evidence of direct threats, criminal terrorist or a threat to national security); those relating to the import and/or export of goods and merchandise to or from the United States; other materials such as books, pamphlets, and printed/manuscript material; monetary instruments; and written materials commonly referred to as "pocket trash" or "pocket litter."

5.3 **Electronic Media.** Any device capable of storing information in digital or analog form. Examples include: hard drives, compact disks, digital versatile disks, flash drives, portable music players, cell phones, pagers, beepers, and video and audio tapes and disks.

5.4 **Letter Class Mail.** U.S. first class mail and its international equivalent. This includes postcards, aerogrammes, letter packets, etc., mailed at the letter class rate or equivalent class or category of postage. To be considered first class mail, a letter must be presently in the U.S. postal system. Only articles presently within the U.S. postal system are deemed "mail," even if they are stamped. Letters that are to be mailed, whether carried or in baggage, are not considered to be letter class mail.

6. **POLICY.** ICE Special Agents acting under border search authority may search, detain, seize, retain, and share documents and electronic media consistent with the guidelines and applicable laws set forth herein. In the course of a border search, and absent individualized suspicion, officers can review the information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States, subject to the requirements and limitations provided herein. Assistance to complete a thorough border search may be sought from outside agencies and entities, on a case by case basis, as appropriate.

NOTE: Nothing in this policy limits the authority of ICE Special Agents to make written notes or reports or to document impressions relating to a border encounter.

7. **RESPONSIBILITIES.**

7.1 The Directors of OI, OPR, and OIA have oversight over the implementation of the provisions of this Directive.

7.2 Special Agents in Charge and Attachés are responsible for implementing the provisions of this Directive and ensuring that their subordinates receive a copy of this Directive and are familiar with its contents.

7.3 Attachés are responsible for ensuring coordination with their host countries and representative Ambassadors, as appropriate, before conducting any such border search outside of the United States.

7.4 ICE personnel are responsible for complying with the provisions of this Directive and must know the limits of ICE authority and use this authority judiciously.

8. PROCEDURES.

8.1 Border Searches by ICE Special Agents.

1) Border searches of documents and electronic media must be performed by an ICE Special Agent or other properly authorized officer with border search authority, such as a CBP Officer or Border Patrol Agent, persons cross designated by ICE as customs officers, and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.

2) At any point during a border search, documents and electronic media, or copies thereof, may be detained for further review, either on-site at the place of detention or at an off-site location, including a location associated with a demand for assistance from an outside agency or entity (see Section 8.4).

3) Except as noted below in Section 8.5(2)(c), if, after reviewing the documents and electronic media, probable cause to seize the documents or electronic media does not exist, all detained copies must be destroyed. Any originals must be returned to the traveler as expeditiously as possible.

8.2 Chain of Custody.

1) Detentions of documents and electronic media. Whenever ICE detains documents or electronic media, or copies thereof, the Special Agent will initiate a chain of custody form (CBP 6051-D) or other appropriate documentation.

2) Seizures of documents and electronic media. Whenever ICE seizes documents or electronic media, or copies thereof, the seizing Special Agent is to enter the seizure into the Seized Asset and Case Tracking System (SEACATS) via the completion of a Search, Arrest, and Seizure Report (SAS). Additionally, the seizing agent must complete the appropriate chain of custody forms (Customs Form 6051) or other appropriate documentation.

8.3 Reasonable Time.

1) ICE personnel are to complete review of any detained or seized documents and electronic media in a reasonable time.

2) ICE Special Agents seeking assistance from other Federal agencies or entities are responsible for ensuring that the results of the review are received in a reasonable time (see Section 8.4(5)).

3) In determining "reasonable time," ICE Special Agents should consider the following factors:

   a) The nature of the documents or electronic media;

   b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;

   c) The elapsed time between the detention, the initial border search, and the continued border search, including any assistance demand;

   d) Whether assistance was sought and the type of such assistance;

   e) Whether ICE followed up with the agency or entity providing assistance to ensure a timely review;

   f) The amount of information needing review; and

   g) Any unanticipated exigency that may arise.

8.4 Assistance by Other Federal Agencies and Non-Federal Entities

1) Translation and Decryption

   a) During a border search, ICE Special Agents may encounter information in documents or electronic media that is in a foreign language and/or encrypted. To assist ICE in determining the meaning of such information, ICE Special Agents may demand translation and/or decryption assistance from other Federal agencies or non-federal entities.

   b) ICE Special Agents may seek such assistance absent individualized suspicion.

   c) ICE Special Agents shall document and record such demands for translation and decryption assistance.

2) Subject Matter Assistance.

   a) During a border search, ICE Special Agents may encounter information in documents or electronic media that are not in a foreign language or encrypted, but that nevertheless require referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by ICE. For the purpose of obtaining such subject matter expertise, ICE Special Agents may create and transmit a copy of information to other Federal agencies or non-federal entities.

   b) ICE Special Agents may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by ICE.

   c) ICE Special Agents shall document and record such demands for subject matter assistance, as appropriate.

3) Originals. For the purpose of obtaining subject matter expertise, ICE Special Agents may create and transmit copies of information to other Federal agencies or non-Federal entities. Any original documents and media should be transmitted only when necessary to render the demanded assistance. If it is not necessary to transmit original documents and media, ICE Special Agents should return originals to the traveler immediately, barring continuing reasonable suspicion to detain.

4) Responses Required.

   a) ICE Special Agents shall inform assisting agencies or entities that they are to provide results of translation and decryption as expeditiously as possible. Additionally, ICE Special Agents shall ensure that assisting agencies and non-federal entities are aware that responses to ICE must include any findings, observations, and conclusions drawn from their review that may relate to the laws enforced by ICE.

   b) If at any time an ICE Special Agent or his/her supervisor are not satisfied with the assistance being provided, the timeliness of assistance, or any other articulable reason, the demand for assistance should be revoked and the ICE Special Agent shall require the assisting agency or non-federal entity to return all documents and electronic media to ICE as expeditiously as possible.

5) Time for Assistance.

   a) Assistance should be accomplished within a reasonable period of time in order to preserve the status of the documents or electronic media and the integrity of the border search.

---

b) It is the responsibility of the ICE Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities. If a demand for assistance is made outside of the Department of Homeland Security, within the first thirty days after demanding the assistance, the ICE Special Agent demanding the assistance shall contact the assisting agency or entity for a status report on the request. If the assisting agency or entity anticipates needing more than thirty days to complete its review and analysis, the ICE Special Agent demanding the assistance shall continue to communicate with the assisting agency or entity on a regular basis until the review is complete and the results have been received. The ICE Special Agent demanding the assistance shall document each communication with the assisting agency or entity. If assisting agencies or entities are not acting in a reasonable time, the ICE Special Agent demanding the assistance shall consult with a supervisor on what action is appropriate.

c) Unless otherwise governed by a Memorandum of Understanding, or similar mechanism, each demand for assistance shall include a letter requesting assistance and detailing the context of the search requested, ICE's legal parameters regarding the search, retention, and sharing, as well as any relevant timeframes, including those described in this section.

8.5 RETENTION, SHARING, SAFEGUARDING AND DESTRUCTION.

1) **By ICE.**

a) Law Enforcement Purposes. When ICE Special Agents determine there is probable cause of unlawful activity—based on a review of information in documents or electronic media or on other facts and circumstances—they may seize and retain the originals and/or copies of relevant documents or electronic media or relevant portions thereof, as authorized by law.

b) Immigration Purposes. To the extent authorized by law, ICE may retain information relevant to immigration matters in ICE record systems. Use, retention, and sharing of such information is governed by the privacy and data protection standards of the system in which such information is retained.

c) Sharing. Copies of documents or electronic media, or portions thereof, which are retained in accordance with this section, may be shared by ICE with Federal, state, local, and foreign law enforcement agencies in accordance with applicable law and policy.

d) Safeguarding Data During Storage and Transmission. ICE will appropriately safeguard information detained, copied, or seized under this directive while in ICE custody and during transmission to an outside entity. Appropriate safeguards include keeping materials in locked cabinets or rooms,

documenting and tracking copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic media or physical protections (e.g., locked containers). Any suspected loss or compromise of information that contains personal data detained, copied, or seized under this directive must be reported immediately to the ICE Help Desk.

e) Destruction. Copies of documents or electronic media, or portions thereof, determined to be of no relevance to ICE will be destroyed. Such destruction must be documented by the responsible ICE Special Agent. Any originals will be returned to the traveler as expeditiously as possible at the conclusion of the negative border search.

2) **By Assisting Agencies and Non-Federal Entities.**

a) Retention During Assistance. All documents and electronic media, whether originals or copies, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to ICE.

b) Return or Destruction. At the conclusion of the requested assistance, all documents and electronic media must be returned to ICE as expeditiously as possible. In the alternative, the assisting Federal agency may certify to ICE that any copies in its possession have been destroyed or it may advise ICE in accordance with Section 8.5(2)(c). In the event that any original documents or electronic media were transmitted, they must not be destroyed; they are to be returned to ICE.

c) Retention with Independent Authority. Copies may be retained by an assisting 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 ICE of its decision to retain certain information on its own authority. In the event that any original documents or electronic media were transmitted, the assisting Federal agency may make a copy for its retention; however, any originals must be returned to ICE.

8.6 Non-Federal Entities.

1) ICE may provide copies of documents or electronic media to an assisting non-federal entity, such as a private language translation or data decryption service, only for the period of time needed by that entity to render the requested assistance.

2) Upon the completion of assistance, all copies of the information in the possession of the entity must be returned to ICE as expeditiously as possible.

8.7 Review and Handling of Certain Types of Information:

1) **Attorney-Client Privilege.**

a) Occasionally, an individual claims that the attorney-client privilege prevents the search of his or her information at the border. Although legal materials are not necessarily exempt from a border search, they may be subject to special handling procedures.

b) Correspondence, court documents, and other legal documents may be covered by attorney-client privilege. If ICE personnel suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the officer must seek advice from the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's office before conducting a search of the document.

2) **Sealed Letter Class Mail.**

a) Border searches of mail are governed by particularized law and policy. *See* 19 C.F.R. Part 145; 19 U.S.C. § 1583. Any possible border search of letter class mail ("LC") shall be coordinated with CBP Officers assigned to such international mail facility and must conform to the guidelines set forth in CBP Handbook 3200-06A, International Mail Operations and Enforcement Handbook, or any successor document. Additionally, the U.S. Postal Service requires that it be notified and present at any border search of LC mail. Consultation with the ICE Office of Chief Counsel or the local U.S. Attorney's Office is recommended when considering a border search of any article that may be considered mail.

b) Letters carried by individuals or private carriers such as DHL, UPS, or Federal Express, for example, are not considered to be mail, even if they are stamped, and thus are subject to border search as provided in this Directive. *See* 19 C.F.R. § 145.3.

3) **Business Information.** If, in the course of a border search, ICE personnel encounter business or commercial information, ICE personnel shall treat such information as business confidential information. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may specifically govern or restrict handling of the information, including criminal penalties for unauthorized disclosure.

4) **Identification and travel documents.** Even without any suspicion of illegality, for legitimate, government purposes, ICE personnel may copy, retain, and share: (1) identification documents such as United States or foreign Passports, Certificates of Naturalization, Seaman's Papers, Airman Certificates, driver's licenses, state identification cards, and similar governmental identification documents, and

(2) travel documents that relate to the person's mode and date of travel into or out of the United States.

9. **ATTACHMENTS.** None.

10. **NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees; or any other person.

Approved Julie L. Myers
Julie L. Myers
Assistant Secretary

U.S. News & WORLD REPORT
Wednesday, June 25, 2008

Seizing Laptops and Cameras Without Cause

A controversial customs practice creates a legal backlash

By Alex Kingsbury
Posted June 24, 2008

Returning from a brief vacation to Germany in February, Bill Hogan was selected for additional screening by customs officials at Dulles International Airport outside Washington, D.C. Agents searched Hogan's luggage and then popped an unexpected question: Was he carrying any digital media cards or drives in his pockets? "Then they told me that they were impounding my laptop," says Hogan, a freelance investigative reporter whose recent stories have ranged from the origins of the Iraq war to the impact of money in presidential politics.

Shaken by the encounter, Hogan says he left the airport and examined his bags, finding that the agents had also removed and inspected the memory card from his digital camera. "It was fortunate that I didn't use that machine for work or I would have had to call up all my sources and tell them that the government had just seized their information," he said. When customs offered to return the machine nearly two weeks later, Hogan told them to ship it to his lawyer.

The extent of the program to confiscate electronics at customs points is unclear. A hearing Wednesday before the Senate Committee on the Judiciary's Subcommittee on the Constitution hopes to learn more about the extent of the program and safeguards to traveler's privacy. Lawsuits have also been filed, challenging how the program selects travelers for inspection. Citing those lawsuits, Customs and Border Protection, a division of the Department of Homeland Security, refuses to say exactly how common the practice is, how many computers, portable storage drives, and BlackBerries have been inspected and confiscated, or what happens to the devices once they are seized. Congressional investigators and plaintiffs involved in lawsuits believe that digital copies—so-called "mirror images" of drives—are sometimes made of materials after they are seized by customs.

A ruling this year by the 9th Circuit Court of Appeals (.pdf) found that DHS does indeed have the authority to search electronic devices without suspicion in the same way that it would inspect a briefcase. The lawsuit that prompted the ruling was the result of more than 20 cases, most of which involved laptops, cellphones, or other electronics seized at airports. In those cases, nearly all of the individuals were of Muslim, Middle Eastern, or South Asian background.

Travelers who have their computers seized face real headaches. "It immediately deprives an executive or company of the very data—and revenue—a business trip was intended to create," says Susan Gurley, head of the Association of Corporate Travel Executives, which is asking DHS for greater transparency and oversight to protect copied data. "As a businessperson returning to the U.S., you may find yourself effectively locked out of your electronic office indefinitely." While Hogan had his computer returned after only a few days, others say they have had theirs held for months at a time. As a result, some companies have instituted policies that require employees to travel with clean machines: free of corporate data.

The security value of the program is unclear, critics say, while the threats to business and privacy are substantial. If drives are being copied, customs officials are potentially duplicating corporate secrets, legal records, financial data, medical files, and personal E-mails and photographs as well as stored passwords for accounts from Netflix to Bank of America. DHS contends that travelers' computers can also contain child pornography, intellectual property offenses, or terrorist secrets.

It makes practical sense to X-ray the contents of checked and carry-on luggage, which could pose an immediate danger to airplanes and their passengers. "Generally speaking, customs officials do not go through briefcases to review and copy paper business records or personal diaries, which is apparently what they are now doing now in digital form—these PDA's don't have bombs in them," says Marc Rotenberg, executive director of the Electronic Privacy Information Center. More troubling is what could happen if other countries follow the lead of the United States. Imagine, for instance, if China or Russia began a program to seize and duplicate the contents of traveler's laptops. "We wouldn't be in a position to strongly object to that type of behavior," Rotenberg says. Indeed, visitors to the Beijing Olympic Games have been officially advised by U.S. officials that their laptops may be targeted for duplication or bugging by Chinese government spies hoping to steal business and trade secrets.

washingtonpost.com

Clarity Sought on Electronics Searches

U.S. Agents Seize Travelers' Devices

By Ellen Nakashima
Washington Post Staff Writer
Thursday, February 7, 2008; A01

Nabila Mango, a therapist and a U.S. citizen who has lived in the country since 1965, had just flown in from Jordan last December when, she said, she was detained at customs and her cellphone was taken from her purse. Her daughter, waiting outside San Francisco International Airport, tried repeatedly to call her during the hour and a half she was questioned. But after her phone was returned, Mango saw that records of her daughter's calls had been erased.

A few months earlier in the same airport, a tech engineer returning from a business trip to London objected when a federal agent asked him to type his password into his laptop computer. "This laptop doesn't belong to me," he remembers protesting. "It belongs to my company." Eventually, he agreed to log on and stood by as the officer copied the Web sites he had visited, said the engineer, a U.S. citizen who spoke on the condition of anonymity for fear of calling attention to himself.

Maria Udy, a marketing executive with a global travel management firm in Bethesda, said her company laptop was seized by a federal agent as she was flying from Dulles International Airport to London in December 2006. Udy, a British citizen, said the agent told her he had "a security concern" with her. "I was basically given the option of handing over my laptop or not getting on that flight," she said.

The seizure of electronics at U.S. borders has prompted protests from travelers who say they now weigh the risk of traveling with sensitive or personal information on their laptops, cameras or cellphones. In some cases, companies have altered their policies to require employees to safeguard corporate secrets by clearing laptop hard drives before international travel.

Today, the Electronic Frontier Foundation and Asian Law Caucus, two civil liberties groups in San Francisco, plan to file a lawsuit to force the government to disclose its policies on border searches, including which rules govern the seizing and copying of the contents of electronic devices. They also want to know the boundaries for asking travelers about their political views, religious practices and other activities potentially protected by the First Amendment. The question of whether border agents have a right to search electronic devices at all without suspicion of a crime is already under review in the federal courts.

The lawsuit was inspired by two dozen cases, 15 of which involved searches of cellphones, laptops, MP3 players and other electronics. Almost all involved travelers of Muslim, Middle Eastern or South Asian background, many of whom, including Mango

and the tech engineer, said they are concerned they were singled out because of racial or religious profiling.

A U.S. Customs and Border Protection spokeswoman, Lynn Hollinger, said officers do not engage in racial profiling "in any way, shape or form." She said that "it is not CBP's intent to subject travelers to unwarranted scrutiny" and that a laptop may be seized if it contains information possibly tied to terrorism, narcotics smuggling, child pornography or other criminal activity.

The reason for a search is not always made clear. The Association of Corporate Travel Executives, which represents 2,500 business executives in the United States and abroad, said it has tracked complaints from several members, including Udy, whose laptops have been seized and their contents copied before usually being returned days later, said Susan Gurley, executive director of ACTE. Gurley said none of the travelers who have complained to the ACTE raised concerns about racial or ethnic profiling. Gurley said none of the travelers were charged with a crime.

"I was assured that my laptop would be given back to me in 10 or 15 days," said Udy, who continues to fly into and out of the United States. She said the federal agent copied her log-on and password, and asked her to show him a recent document and how she gains access to Microsoft Word. She was asked to pull up her e-mail but could not because of lack of Internet access. With ACTE's help, she pressed for relief. More than a year later, Udy has received neither her laptop nor an explanation.

ACTE last year filed a Freedom of Information Act request to press the government for information on what happens to data seized from laptops and other electronic devices. "Is it destroyed right then and there if the person is in fact just a regular business traveler?" Gurley asked. "People are quite concerned. They don't want proprietary business information floating, not knowing where it has landed or where it is going. It increases the anxiety level."

Udy has changed all her work passwords and no longer banks online. Her company, Radius, has tightened its data policies so that traveling employees must access company information remotely via an encrypted channel, and their laptops must contain no company information.

At least two major global corporations, one American and one Dutch, have told their executives not to carry confidential business material on laptops on overseas trips, Gurley said. In Canada, one law firm has instructed its lawyers to travel to the United States with "blank laptops" whose hard drives contain no data. "We just access our information through the Internet," said Lou Brzezinski, a partner at Blaney McMurtry, a major Toronto law firm. That approach also holds risks, but "those are hacking risks as opposed to search risks," he said.

The U.S. government has argued in a pending court case that its authority to protect the country's border extends to looking at information stored in electronic devices such as

laptops without any suspicion of a crime. In border searches, it regards a laptop the same as a suitcase.

"It should not matter . . . whether documents and pictures are kept in 'hard copy' form in an executive's briefcase or stored digitally in a computer. The authority of customs officials to search the former should extend equally to searches of the latter," the government argued in the child pornography case being heard by a three-judge panel of the Court of Appeals for the 9th Circuit in San Francisco.

As more and more people travel with laptops, BlackBerrys and cellphones, the government's laptop-equals-suitcase position is raising red flags.

"It's one thing to say it's reasonable for government agents to open your luggage," said David D. Cole, a law professor at Georgetown University. "It's another thing to say it's reasonable for them to read your mind and everything you have thought over the last year. What a laptop records is as personal as a diary but much more extensive. It records every Web site you have searched. Every e-mail you have sent. It's as if you're crossing the border with your home in your suitcase."

If the government's position on searches of electronic files is upheld, new risks will confront anyone who crosses the border with a laptop or other device, said Mark Rasch, a technology security expert with FTI Consulting and a former federal prosecutor. "Your kid can be arrested because they can't prove the songs they downloaded to their iPod were legally downloaded," he said. "Lawyers run the risk of exposing sensitive information about their client. Trade secrets can be exposed to customs agents with no limit on what they can do with it. Journalists can expose sources, all because they have the audacity to cross an invisible line."

Hollinger said customs officers "are trained to protect confidential information."

Shirin Sinnar, a staff attorney with the Asian Law Caucus, said that by scrutinizing the Web sites people search and the phone numbers they've stored on their cellphones, "the government is going well beyond its traditional role of looking for contraband and really is looking into the content of people's thoughts and ideas and their lawful political activities."

If conducted inside the country, such searches would require a warrant and probable cause, legal experts said.

Customs sometimes singles out passengers for extensive questioning and searches based on "information from various systems and specific techniques for selecting passengers," including the Interagency Border Inspection System, according to a statement on the CBP Web site. "CBP officers may, unfortunately, inconvenience law-abiding citizens in order to detect those involved in illicit activities," the statement said. But the factors agents use to single out passengers are not transparent, and travelers generally have little access to the data to see whether there are errors.

Although Customs said it does not profile by race or ethnicity, an officers' training guide states that "it is permissible and indeed advisable to consider an individual's connections to countries that are associated with significant terrorist activity."

"What's the difference between that and targeting people because they are Arab or Muslim?" Cole said, noting that the countries the government focuses on are generally predominantly Arab or Muslim.

It is the lack of clarity about the rules that has confounded travelers and raised concerns from groups such as the Asian Law Caucus, which said that as a result, their lawyers cannot fully advise people how they may exercise their rights during a border search. The lawsuit says a Freedom of Information Act request was filed with Customs last fall but that no information has been received.

Kamran Habib, a software engineer with Cisco Systems, has had his laptop and cellphone searched three times in the past year. Once, in San Francisco, an officer "went through every number and text message on my cellphone and took out my SIM card in the back," said Habib, a permanent U.S. resident. "So now, every time I travel, I basically clean out my phone. It's better for me to keep my colleagues and friends safe than to get them on the list as well."

Udy's company, Radius, organizes business trips for 100,000 travelers a day, from companies around the world. She says her firm supports strong security measures. "Where we get angry is when we don't know what they're for."

Staff researcher Richard Drezen contributed to this report.