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).