

*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)