



**GEORGE
MASON**
UNIVERSITY

School of Law

RUN FOR THE BORDER: LAPTOP SEARCHES AND THE FOURTH AMENDMENT

**Nathan A. Sales,
George Mason University School of Law**

**George Mason University Law and Economics
Research Paper Series**

08-58

This paper can be downloaded without charge from the Social Science
Research Network at http://ssrn.com/abstract_id=1279683

RUN FOR THE BORDER:
LAPTOP SEARCHES AND THE FOURTH AMENDMENT

Nathan Alexander Sales

ABSTRACT

Should customs officers be able to search laptop computers at the border in the same way they inspect suitcases and packages? This article argues that, in general, suspicionless border searches of laptops and other electronic storage devices are permissible under the Fourth Amendment. It begins by surveying the competing interests that are implicated by laptop searches at the border, including the government’s need to combat terrorism and child exploitation, as well as travelers’ interests in privacy and free expression. Next, the article discusses the Supreme Court’s border-search doctrine. “Non-routine” border searches (e.g., invasive searches of the body) are subject to the reasonable-suspicion standard, but “routine” searches (e.g., searches of property) need not be based on any individualized suspicion at all. The article then considers how the border-search doctrine might apply to laptops. Lower courts generally hold that customs can inspect laptops without reasonable suspicion, and this consensus is largely correct. Laptops differ from other kinds of property: They contain a greater volume of material, the data they store is intensely personal, and digital searches can leave a permanent copy of the data in the government’s hands. But those differences generally do not justify a special exception to the border-search doctrine. In fact, laptop searches have the potential to be less, not more, intrusive than traditional border inspections of physical objects. Finally, the article discusses possible legislative or administrative reforms that might better balance travelers’ interests against the government’s needs. It might be appropriate to protect laptop owners’ privacy interests at the border, not through traditional “collection limits” (which restrict the government’s ability to gather information in the first place), but with “use limits” (which restrict the government’s ability to share or otherwise use the information it does gather).

RUN FOR THE BORDER:
LAPTOP SEARCHES AND THE FOURTH AMENDMENT

Nathan Alexander Sales[†]

TABLE OF CONTENTS

Introduction.....	1
I. The Competing Interests of Laptop Searches	3
II. The Supreme Court’s Border-Search Caselaw.....	8
III. Laptop Searches Under the Fourth Amendment	11
A. Laptops in Court	12
B. A Special Rule for Laptops?.....	13
C. Intrusiveness Reconsidered	19
IV. Additional Protections: Collection Limits vs. Use Limits	21
Conclusion	26

INTRODUCTION

On May 27, 1998, a man named Stefan Irving flew from Mexico to Dallas-Fort Worth International Airport. Formerly the chief pediatrician for a New York school district, Irving’s license to practice medicine was stripped after a 1983 conviction for “attempted sexual abuse in the first degree of a seven-year old boy.”¹ He served his time – 16 to 48 months in prison – and was released. Now he was returning home from what was by all lights a typical vacation in Acapulco.

Customs officers at Dallas knew that Irving was a convicted pedophile, and they decided to search his luggage. They 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.” When the disks were analyzed, they were found to contain “[i]mages of child erotica.”² A subsequent search of the computer in Irving’s Brooklyn apartment uncovered 76 video files of “boys engaging in various sexual acts with each other and in other cases of sexual acts by themselves.”³

[†] Assistant Professor of Law, George Mason University School of Law. This article is based on testimony I gave before the United States Senate. *See Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing the Subcomm. on the Constitution, Civil Rights and Property Rights of the S. Comm. on the Judiciary*, 110th Cong (2008).

¹ *United States v. Irving*, 452 F.3d 110, 114 (2d Cir. 2006).

² *Id.*

³ *Id.* at 116.

Investigators later determined that the reason Irving traveled to Mexico was to visit “a guest house that served as a place where men from the United States could have sexual relations with Mexican boys.”⁴ Irving “preferred prepubescent boys, under the age of 11.”⁵

Stefan Irving is now back in prison, serving a 262-month sentence for possession of child pornography, traveling outside the United States to engage in sexual acts with children, and other crimes.⁶ We justifiably applaud the incapacitation of child predators. But the border search that helped lead to Irving’s conviction raises some vexing problems. When told that the government claims the power to rummage through travelers’ laptops, BlackBerries, and flash drives at the border, many people react with shock, even revulsion. A laptop search seems terribly invasive. The most intimate details of one’s life – emails to friends and colleagues, family photographs, financial records, and so on – are paraded in front of the officer at the customs checkpoint. The average traveler may be willing to hand over his suitcase for inspection, but his laptop seems a bridge too far.

This article considers a number of questions that arise out of the government’s occasional practice of inspecting laptop computers and other electronic media at the border. For instance, should customs officers at the Department of Homeland Security be able to search a laptop without any individualized suspicion that its owner is up to no good? Or should such inspections be off-limits unless officers are able to establish reasonable suspicion, or maybe even demonstrate probable cause and obtain a judicial warrant? Do searches of laptop computers present unique problems that aren’t present when border officials inspect suitcases, packages, and other types of property? If so, do those differences justify a different Fourth Amendment standard for laptop searches?

I argue that suspicionless border searches of laptop computers and other electronic devices generally are permissible under the Fourth Amendment. Part I examines the range of compelling, and often competing, interests that are implicated by border inspections of laptops. Those interests include the government’s need to detect terrorists crossing our borders and to combat child exploitation, as well as law-abiding travelers’ equally weighty interests in personal privacy and free expression. In Part II, I discuss the Supreme Court’s border-search doctrine. According to the Court, “non-routine” border searches (e.g., invasive searches of the body) are subject to the reasonable-suspicion standard, but “routine” searches (e.g., searches of property) need not be preceded by any individualized suspicion whatsoever. Routine searches satisfy the Fourth Amendment’s reasonableness requirement simply by virtue of the fact that they occur at the border.

Part III considers how the border-search doctrine might apply to the particular problem of laptop computers. The consensus among lower federal courts is that a laptop search counts as routine; customs officers therefore don’t need to have reasonable suspicion before inspecting a particular traveler’s computer. My sense is that the courts are getting it right. Laptops are in fact different from other types of property: They potentially contain much more personal data than

⁴ *Id.* at 114.

⁵ *Id.* at 115.

⁶ *See id.* at 113.

other items that cross the border; the information they do contain can be quite sensitive and revealing (e.g., photo albums, emails, records of the owner’s web browsing); and officers often inspect laptops by copying their hard drives, raising the possibility that the government might keep the data for long periods of time, perhaps indefinitely. But while laptops are different, those differences don’t justify a blanket “laptop exception” to the border-search doctrine. In fact, laptop inspections have the potential to be less, not more, intrusive than traditional border searches of physical objects. With laptop searches, automated and impersonal computer processes (like keyword searches) can identify specific data points that might warrant further investigation, eliminating the need for customs officers to sift through the bulk information manually. Finally, Part IV discusses legislative or administrative reforms that might better balance travelers’ privacy interests against Homeland Security’s counterterrorism and law-enforcement needs. While the Fourth Amendment imposes few restrictions on laptop searches, policymakers might wish to implement other safeguards that supplement these relatively weak constitutional protections. More specifically, it might be appropriate to protect laptop owners’ privacy interests at the border, not through traditional “collection limits” (which restrict the government’s ability to gather information in the first place), but with “use limits” (which restrict the government’s ability to share or otherwise use the information it does gather).

This article self consciously has modest aims. It does not comprehensively address the thorny problems that arise whenever the government searches data stored in electronic format⁷; it is content to focus on one particular manifestation of that problem – electronic searches at the border. Similarly, this article does not attempt to trace the history of the border-search doctrine from the founding era to the modern day. Nor does it mount an independent defense of the doctrine on originalist, normative, or other grounds. Instead, it simply assumes that the border-search doctrine is sound and considers how it might apply to inspections of laptop computers and other electronic storage devices. The question I ask is not *Should we have a border-search doctrine?*, but rather *Given that we have a border-search doctrine, what should it say about laptops?*

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. For terrorists, the ability to travel is “as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To them, international travel presents great danger, because they must surface to pass through regulated channels, present themselves to border security officials, or attempt to circumvent entry points.”⁸ 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 is said to have stored incriminating data on his laptop computer, including

⁷ See generally Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

⁸ NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 384 (2004).

information about crop-dusting aircraft and wind patterns.⁹ If investigators had found these clues on his laptop when he arrived in the United States in February 2001, they might have begun to unravel his ties to al Qaeda.¹⁰ We should be careful not to overstate the case. Seven years have passed since 9/11, and uncertainty still lingers over exactly what Moussaoui had on his computer. Nor is it clear that the laptop had any incriminating data when he crossed the border into this country, or that investigators would have been able to use that information to identify other al Qaeda operatives in the U.S. Still, it seems possible that a border search of Moussaoui's computer might have uncovered clues that could have shed some light on the September 11 plot.

More recently, in 2006, a laptop search at Minneapolis-St. Paul airport helped U.S. Customs and Border Protection (a division of the Department of Homeland Security) detect a potentially risky traveler. Once he was referred to secondary inspection, officers 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.¹¹ Government officials have claimed other counterterrorism victories, as well:

During border searches of lap tops [sic] 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. [sic] and its citizens. These materials have led to the refusal admission [sic] and the removal of these dangerous people from the United States.¹²

This account is as regrettably short on details as it is painfully long on typos. Perhaps its brevity is due to the government's fear that publicity about its national-security operations might alert terrorists how to avoid detection. Whatever the reason, the absence of more detail makes it difficult to know how much weight to assign to these incidents. Yet it's not much of a stretch to say that laptop searches have the potential to reveal terrorist operatives, financiers, and handlers, even if their successes to date are somewhat ambiguous.

⁹ 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.

¹⁰ For a discussion of the FBI's failure to obtain judicial authorization to search Moussaoui's laptop after his August 16, 2001 arrest on immigration charges, see Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951, 957-72 (2003); see also 9/11 COMMISSION REPORT, *supra* note 8, at 276 ("A maximum U.S. effort to investigate Moussaoui conceivably could have unearthed his connections to [Ramzi] Binalshibh. Those connections might have brought investigators to the core of the 9/11 plot.").

¹¹ See Remarks of Stewart A. Baker, Assistant Secretary for Policy, U.S. Dep't of Homeland Security, at the Center for Strategic and Int'l Studies, Dec. 19, 2006.

¹² *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution, Civil Rights and Property Rights of the S. Comm. on the Judiciary*, 110th Cong. (2008) (statement of Jayson P. Ahern, Deputy Commissioner, U.S. Customs and Border Protection).

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. As of this writing, there have been twelve federal decisions examining the scope of the government’s authority to search laptops at the border, and every single one has involved child pornography. Unfortunately, Stefan Irving is far from an anomaly.

For instance, 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.”¹³ 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.”¹⁴ In 2000, 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.”¹⁵

Of course, laptops are not the only way to smuggle contraband into the United States. Moderately sophisticated terrorists and child predators could accomplish the same thing by uploading materials to a private server, or emailing encrypted files to themselves, and then accessing the data once they have entered the country. It has been suggested that the existence of these alternative pathways makes laptop searches ineffective (and maybe even constitutionally unreasonable).¹⁶ Yet the fact that terrorists and others might use a number of techniques to commit their crimes does not diminish the magnitude of the government’s interest in inhibiting this particular technique. Narcotics dealers might smuggle illegal drugs into the United States via FedEx or UPS, and they might produce narcotics within the United States. But that doesn’t make it futile (or unconstitutional) for customs officers to search suspected balloon swallows in appropriate circumstances. Laptop searches may not be a perfectly effective way of interdicting contraband or detecting terrorist threats, but they don’t have to be.

A final word on the government’s interests: The need to detect terrorists and child predators *entering* the country is fairly intuitive, but the government also may have good reasons to search *outbound* travelers. One might think that the need to prevent the departure of security

¹³ United States v. Ickes, 393 F.3d 501, 503 (4th Cir. 2005).

¹⁴ United States v. Hampe, Crim. No. 07-3-B-W, 2007 WL 1192365, at *2 (D. Me. April 18, 2007).

¹⁵ United States v. McAuley, No. DR-07-CR-786(1)-AML, 2008 WL 2387979, at *2 (W.D. Tex. June 6, 2008).

¹⁶ See *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution, Civil Rights and Property Rights of the S. Comm. on the Judiciary*, 110th Cong. (2008) (statement of Peter P. Swire, C. William O’Neill Professor of Law, Moritz College of Law, The Ohio State University) (arguing that “these approaches show the inability of laptop border searches to catch moderately smart criminals or terrorists,” and that “a system that can be evaded by competent criminals but imposes large costs on honest citizens should be avoided”); Rasha Alzahabi, Note, *Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers*, 41 IND. L.J. 161, 175 (2008) (“The information saved on a laptop can be transported into our country electronically, regardless of whether the traveler or the laptop crosses the border.”).

threats is less compelling; a terrorist who is not in the United States cannot attack the United States. Yet the government still might have an interest in detecting terrorist exits. Operatives might be leaving the country to receive training, funding, or direction, and a laptop search might reveal the identities of previously unknown associates overseas. They might be leaving to attack outbound international flights; a search at departure could help disrupt the plot. Likewise, one might think that the removal of child pornography from this country does not harm – and may even vindicate – the government’s interests in excluding contraband from the United States. Yet the government might wish to inspect outbound laptops as a *quid pro quo* for other countries acting to stem the flow of child pornography from their territories. Outbound laptop searches also can help the government enforce export control laws against the removal of sensitive technologies (including software), and prevent the transmission of classified information to hostile powers overseas. In short, the government’s interests are at their zenith at the passport-control booth, but they are not nonexistent at the departure gate.¹⁷

While the government’s interest in combating terrorism and child exploitation are significant, 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.”¹⁸ 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.¹⁹

¹⁷ This is not to say that the government’s interest is necessarily conclusive, or that exit searches should be judged by the same reasonable-suspicion standard that applies to most entry searches. The Supreme Court has suggested in dicta that entry and exit searches are equally permissible. See *California Bankers Ass’n v. Schultz*, 416 U.S. 21, 63 (indicating that “those entering and leaving the country may be examined as to their belongings and effects, all without violating the Fourth Amendment”) (1974); see also Larry Cunningham, *The Border Search Exception as Applied to Exit and Export Searches: A Global Conception*, 26 QUINNIPIAC L. REV. 1, 2 (2007) (arguing that “routine suspicionless and warrantless searches of exiting individuals and property are inherently ‘reasonable’ under the Fourth Amendment”). Yet a number of judges and academics have questioned whether the Fourth Amendment permits officials to conduct suspicionless searches of persons or property leaving the country. See, e.g., *United States v. Nates*, 831 F.2d 860, ___ (1987) (Kozinski, J., dissenting) (arguing that suspicionless exit searches are unreasonable under the Fourth Amendment); Abraham Abramovsky, *Money-Laundering and Narcotics Prosecution*, 54 FORDHAM L. REV. 471, 503-04 (1986) (arguing that border officials should be required to demonstrate probable cause and obtain a warrant before conducting an exit search); John Rogers, *Bombs, Borders, and Boarding: Combating International Terrorism at United States Airports and the Fourth Amendment*, 20 SUFFOLK TRANSNAT’L L. REV. 501, 518 (1997) (“The traditional argument that border searches are reasonable simply by virtue of occurring at the border may not be a sufficient basis on which to support exit searches.”). I take no sides in this dispute. My purpose here is simply to suggest that the government has some interest, however much weight we ultimately give it, in conducting effective exit searches.

¹⁸ Nathan Alexander Sales, *Secrecy and National Security Investigations*, 58 ALA. L. REV. 811, 823 (2007).

¹⁹ 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”).

Laptops can contain massive amounts of information. A modern-day 250-gigabyte hard drive is capable of storing the equivalent of 125 million printed pages of text. It would only take 63 such devices to store the entire collection of the Library of Congress.²⁰ Even a now-archaic 80-gigabyte hard drive boasts an impressive storage capacity: 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.”²¹

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 simultaneously can be 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. Physicians might store the medical records of hundreds of patients. And lawyers’ computers might have materials covered by the attorney-client privilege. For these reasons, Professor David Cole has likened searches of computers to searches of 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.”²²

Border searches don’t just threaten privacy interests. They also have the potential to harm travelers’ interests in free expression. Laptop computers often contain significant amounts of expressive material – correspondence with friends and colleagues about the hot-button issues of the day; records of the internet content the owner has accessed; membership lists for political or other advocacy groups; transactional records of the books the owner has ordered from Amazon.com; financial records indicating the causes and religious organizations to which the owner has contributed; and so on. If a traveler knows his expressive activities could be exposed to the government’s prying eye when he crosses the border, he might be chilled from engaging in those activities in the first place.²³ At a minimum, he might refrain from engaging in them with his computer. Laptop inspections thus “reflect a convergence of First and Fourth Amendment values.”²⁴

Searches of laptops also can place real strain on the right to travel. Business travelers and tourists alike might be reluctant to take to the skies if they fear that border officials will rifle through their electronic data. At a minimum, they may leave their computers behind when they travel, or they might carry sanitized “travel laptops” on the road, but those workarounds might not be a realistic option for some. In a sense, this is the flip side of the free-expression coin. People who can’t realistically minimize their expressive activities (e.g., journalists, opinion leaders, and activists) might cope with border searches by minimizing their overseas travel. People who can’t realistically minimize their overseas travel (e.g., global businessmen) might cope with border

²⁰ See Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 144 (2008).

²¹ See Kerr, *supra* note 7, at 542.

²² Quoted in Ellen Nakashima, *Clarity Sought on Electronics Searches*, WASH. POST, Feb. 7, 2008, at A01.

²³ Cf. NAACP v. Alabama, 357 U.S. 449, ___ (1958).

²⁴ United States v. United States District Court, 407 U.S. 297, ___ (1972) (“Keith”).

searches by minimizing their expressive activities. Either way, there is a risk that core constitutional values will be chilled.

II. THE SUPREME COURT’S BORDER-SEARCH CASELAW

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 judicial warrant before conducting a search,²⁵ the Supreme Court began to carve out an exception for border searches as early as 1886.²⁶ In 1977, the Court made it official. *Ramsey v. United States* squarely held that “border searches were not subject to the warrant provisions of the Fourth Amendment and were ‘reasonable’ within the meaning of that Amendment.”²⁷ According to the Court, “[s]ince 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 contraband into this country.”²⁸

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.”²⁹ For routine inspections, officers don’t need to have any suspicion whatsoever, reasonable or otherwise. The Fourth Amendment permits them to conduct “*suspicionless*” searches.³⁰ This is not to suggest that the Fourth Amendment’s reasonableness requirement doesn’t apply at the border. It does.³¹ But border searches are deemed “reasonable simply by virtue of the fact that they occur at the border.”³²

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

²⁵ See, e.g., *Katz v. United States*, 389 U.S. 347, 357 (1967).

²⁶ See *Boyd v. United States*, 116 U.S. 616, 623 (1886); see also *Carroll v. United States*, 267 U.S. 132, 154 (1925). For histories of the Supreme Court’s border-search caselaw, see Cunningham, *supra* note 17, at 3-15; Kelly A. Gilmore, Note, *Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border*, 72 BROOKLYN L. REV. 759, 764-69 (2007); Harris J. Yale, Note, *Beyond the Border of Reasonableness: Exports, Imports and the Border Search Exception*, 11 HOFSTRA L. REV. 733, 736-45 (1983).

²⁷ 431 U.S. 606, 617 (1977).

²⁸ *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985).

²⁹ *Id.* at 538; see also *id.* at 551 (Brennan, J., dissenting) (agreeing that “thorough searches of [travelers’] belongings . . . do not violate the Fourth Amendment”).

³⁰ *Flores-Montano*, 541 U.S. at 154 (emphasis added).

³¹ *Contra* *Abramovsky*, *supra* note 17, at 483 (“The border search exception is actually an exception to the fourth amendment itself and not to the amendment’s probable cause or warrant requirements.”).

³² *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.’”).

as carrying contraband.³³ 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 x-ray examinations.³⁴ 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.”³⁵ Searches of the body are more invasive than searches of belongings, and the Court therefore insists that officers have a measure of individualized suspicion before conducting them.

Two cases help illustrate the differences between routine and non-routine inspections. The first, *United States v. Flores-Montano*, involved a suspicionless search of a station wagon that was crossing into California from Mexico. Customs inspectors tapped on the car’s gas tank and noticed it sounded solid. They called a mechanic, who removed the tank. When it was opened, investigators found about 80 pounds of marijuana.³⁶ A unanimous Supreme Court upheld the inspection as a legitimate routine border search. According to the Court, neither the defendant’s asserted privacy interest in his gas tank, nor the possibility that disassembling the tank might damage his property, made the search constitutionally unreasonable.³⁷ Instead, invoking “the Government’s paramount interest in protecting the border,” the Court concluded that “the Government’s authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle’s fuel tank.”³⁸

The second case, *United States v. Montoya de Hernandez*, is a particularly evocative example of non-routine border inspections. Shortly after midnight, Montoya de Hernandez arrived at Los Angeles International Airport on a flight from Bogota, Colombia. Examining her passport, customs officers noticed that she had traveled to Los Angeles or Miami on at least eight recent occasions. Further questioning revealed that she had no friends or family in the United States; she was carrying \$5,000 in cash; she had no hotel reservations; and she could not say how her plane ticket had been purchased.³⁹ The officers suspected that she was a “balloon swallower,” smuggling drugs in her alimentary canal, so they detained her. She was given the choice of returning to Colombia on the next available flight (which did not leave for a number of hours), submitting to an x-ray (she initially agreed, but then withdrew consent), or using a wastebasket to “produce a monitored bowel movement that would confirm or rebut the inspectors’ suspicions”⁴⁰ (she refused, and would come to “exhibit[] symptoms of discomfort consistent with heroic efforts to resist the usual calls of nature”⁴¹). Nature eventually won.

³³ 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).

³⁴ See *Montoya de Hernandez*, 473 U.S. at 541 n.4.

³⁵ *Flores-Montano*, 541 U.S. at 152.

³⁶ See *id.* at 150-51.

³⁷ See *id.* at 154.

³⁸ *Id.* at 155.

³⁹ See *Montoya de Hernandez*, 473 U.S. at 533-34.

⁴⁰ *Id.* at 534-35.

⁴¹ *Id.* at 535 (citation and internal quotation marks omitted).

After more than 16 hours in custody, Montoya de Hernandez “passed 88 balloons containing a total of 528 grams of 80% pure cocaine hydrochloride.”⁴²

A divided Supreme Court upheld her detention as reasonable under the Fourth Amendment. According to the majority, non-routine “detention of a traveler at the border” – i.e., detention “beyond the scope of a routine customs search and inspection” – is justified if officers “reasonably suspect that the traveler is smuggling contraband in her alimentary canal.”⁴³ If the government wants to engage in non-routine border detention, it needs more particularized suspicion than is necessary to justify the initial routine search (namely, no suspicion whatsoever), but it is not required to establish probable cause or obtain a judicial warrant. It bears emphasis that *Montoya de Hernandez* is a seizure case, not a search case. But it still offers important insights into the Court’s understanding of what counts as a non-routine search.⁴⁴

What is the legal basis for the border-search doctrine? In part, the doctrine rests on originalist grounds. Exhibit A in the Supreme Court’s case for border searches is a statute Congress enacted in 1789, which granted 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.” By contrast, customs could search a “dwelling-house, store, building, or other place” only after obtaining a warrant.⁴⁵ Because Congress enacted the law a mere two months before sending what would become the Fourth Amendment to the states for ratification, the Court has regarded it as evidence that the founding generation viewed border inspections as constitutionally permissible.⁴⁶ “This analysis has been nearly universally accepted by the judiciary.”⁴⁷

⁴² *Id.* at 536.

⁴³ *Id.* at 541.

⁴⁴ *See id.* at 542 n.4 (declining to express any “view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches”). Later, the Court would suggest that non-routine border searches must be based on reasonable suspicion. *See Flores-Montano*, 541 U.S. at 152.

⁴⁵ Act of July 31, 1789, c. 5, § 24, 1 Stat. 29. The full text of the statute is as follows:

That every collector, naval officer and surveyor, or other person specially appointed by either of them for that purpose, shall have full power and authority, to enter any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed; and therein to search for, seize, and secure any such goods, wares or merchandise; and if they shall have cause to suspect a concealment thereof, in any particular dwelling-house, store, building, or other place, they or either of them shall, upon application on oath or affirmation to any justice of the peace, be entitled to a warrant to enter such house, store, or other place (in the day time only) and there to search for such goods, and if any shall be found, to seize and secure the same for trial; and all such goods, wares and merchandise, on which the duties shall not have been paid or secured, shall be forfeited.

⁴⁶ *See, e.g.,* *United States v. Ramsey*, 431 U.S. 606, __ (1977) (__); *Boyd v. United States*, 116 U.S. 616, 623 (1886) (emphasizing that the 1789 act “was passed by the same Congress that proposed for adoption the original amendments to the Constitution,” and therefore concluding that “the members of that body did not regard searches and seizures of this kind as ‘unreasonable,’ and they are not embraced within the prohibition” of the Fourth Amendment).

⁴⁷ Yale, *supra* note 26, at 744.

Yet the originalist defense is far from airtight. The 1789 statute did not require probable cause or warrants for vessel searches, but neither does it appear to have authorized the suspicionless searches associated with modern-day routine border inspections. Instead, it permitted searches only when there was “*reason to suspect*” lawbreaking – a close cousin of the reasonable-suspicion standard that applies to non-routine searches. (Of course, “reason to suspect” is not identical to “reasonable suspicion.” A customs inspector’s reason to suspect the presence of contraband may be constitutionally unreasonable – for example, if based on the race or ethnicity of the ship’s captain.) Scholars have pointed out other flaws.⁴⁸

The Supreme Court also has grounded border searches in considerations of public policy and legal doctrine. The power to conduct suspicionless inspections at the border is said to derive from the “inherent authority” of the United States “as sovereign” to “protect . . . its territorial integrity.”⁴⁹ The government likewise has a “paramount interest” in keeping dangerous people and items on the other side of border.⁵⁰ The magnitude of these governmental interests is reinforced by the diminished expectations of privacy held by international travelers.⁵¹ At times, the Court stresses a legal theory of the (pre-constitutional?) origins of the government’s search powers; at times it stresses the policy advantages that flow from embracing that theory. The two sets of considerations thus tend to merge: The government may search because it needs to protect the border and because its power to do so is a necessary concomitant of nationality. Again, not all scholars are persuaded that these considerations justify the border-search doctrine.⁵²

III. LAPTOP SEARCHES UNDER THE FOURTH AMENDMENT

⁴⁸ For instance, Harris Yale emphasizes that the border-search law was enacted before Congress considered the Bill of Rights; “[s]ince the debate on the parameters of an unreasonable search had not yet occurred, it cannot be said that such searches were considered reasonable by Congress.” Yale, *supra* note 26, at 746. He also argues that, given widespread colonial outrage over writs of assistance (which authorized customs officers “to search wherever they suspected uncustomed goods to be”), it is “improbable that Congress would ignore the lessons of recent history and restore, even in limited circumstances, the power of the writs of assistance with their objectionable prerogatives.” *Id.* at 739, 747-48 (footnote omitted); *see also, e.g.*, Judith B. Ittig, *The Rites of Passage: Border Searches and the Fourth Amendment*, 40 TENN. L. REV. 329, 333 (1973) (arguing that “[t]he standard of reasonableness . . . has been continually restructured to accommodate changing community standards with respect to the privacy and dignity of the individual”); Note, *Border Searches and the Fourth Amendment*, 77 YALE L.J. 1007, 1011 (1968) (arguing that history “is not dispositive,” partly because Congress may have enacted the statute without considering how it might relate to the Fourth Amendment, and partly because the nation’s “standards of reasonableness may have changed over time”).

⁴⁹ *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004).

⁵⁰ *Id.* at 155.

⁵¹ CITE.

⁵² *See* 3 LaFave § 10.5, at 325 (objecting that the Supreme Court has offered “a flimsy and not particularly satisfying explanation” of the border-search doctrine); Note, *supra* note 48, at 1011-12 (concluding that the “special conditions prevailing at the border . . . do not by themselves justify the current border search exception”); Yale, *supra* note 26, at 759 (“Given the possibility and severity of criminal penalties resulting from evidence discovered during border searches, fourth amendment protection in the form of probable cause as the minimum requirement for a border search is a must.” (footnote omitted)).

As I have said, this is not the place to resolve whether or not the border-search doctrine is sound. It is enough for our purposes simply to acknowledge that it exists. The question then becomes whether a laptop inspection at the border 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. Those decisions are probably correct. A number of important differences exist between laptop computers and other types of property, but those differences do not justify a blanket “laptop exception” to the border-search doctrine.⁵³ In fact, laptop searches have the potential to be *less* intrusive than traditional border searches of travelers and their goods.

A. *Laptops in Court*

As of this writing there have been twelve federal decisions applying the Supreme Court’s border-search precedents to laptop computers and other electronic storage devices. Eight of the twelve hold or imply that customs officials may search laptops at the border with no particularized suspicion at all: The Third Circuit, Fourth Circuit, Ninth Circuit (twice), District of Maine, Eastern District of Pennsylvania, Southern District of Texas, and Western District of Texas.⁵⁴ 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.⁵⁵ Other than a single California district court that was reversed on appeal,⁵⁶ 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.

Thus far the Supreme Court has been content to watch the action from the sidelines, and it may not have much enthusiasm for disturbing this lower-court consensus. For starters, the Court on at least two prior occasions has declined invitations to extend the more rigorous

⁵³ 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 laptop searches at the border, “as a matter of practice, we only do it where there’s a reasonable suspicion.” Testimony of Michael Chertoff, Secretary, United States Department of Homeland Security, Before the United States Senate Committee on the Judiciary, Apr. 2, 2008.

⁵⁴ See *United States v. Linarez-Delgado*, 259 Fed. Appx. 506, 507-08 (3d Cir. 2007); *United States v. Ickes*, 393 F.3d 501, 505 & n.1 (4th Cir. 2005); *United States v. Arnold*, 523 F.3d 941, 948 (9th Cir. 2008); *United States v. Hampe*, Crim. No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. April 18, 2007); *United States v. Bunty*, Crim. No. 07-641, 2008 WL 2371211, at *3 (E.D. Pa. June 10, 2008); *United States v. Roberts*, 86 F. Supp. 2d 678, 688-89 (S.D. Tex. 2000), *aff’d*, 274 F.3d 1007 (5th Cir. 2001); *United States v. McAuley*, No. DR-07-CR-786(1)-AML, 2008 WL 2387979, at *4-6 (W.D. Tex. June 6, 2008); *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).

⁵⁵ 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).

⁵⁶ See *United States v. Arnold*, 454 F. Supp. 2d 999 (C.D. Cal. 2006), *rev’d*, 523 F.3d 941 (9th Cir. 2008).

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 considerations, requiring the full panoply of Fourth Amendment protections, apply to international mail.”⁵⁷ Likewise, in *United States v. Flores-Montano*, a unanimous Court denied that border searches involving the disassembly of (and hence the potential for damage to) vehicles required reasonable suspicion.⁵⁸ 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. As property, a laptop falls on the other side of the line.

B. A Special Rule for Laptops?

A laptop is a piece of property, but there’s property and then there’s property. Laptop computers differ from other items subject to routine border searches in at least three potentially relevant ways.⁵⁹ First, laptops usually store vastly more content than, say, a suitcase or a package of goods. Second, the material kept on a laptop often will be more personal and sensitive than other types of property. Third, the government often searches a laptop by mirroring its hard drive, which raises the possibility that it might retain a permanent copy of the extracted data. Do any of these differences justify adopting a special rule for border searches of laptops? In general, no.

Amount of information. Because laptop computers potentially contain massive amounts of data – far more content than the typical traveler carries when crossing the border – it has been suggested that courts should fashion a special rule for laptop searches. One student note argues for a reasonable-suspicion standard in part because laptops “may contain an immense amount of information.”⁶⁰ Yet for reasons of history and policy, it is inadvisable to distinguish among containers based on the amount of content they can carry. Size doesn’t matter.

First, consider history. The 1789 border-search statute gave customs officers blanket authority to inspect “any vessel” that might contain goods subject to duty.⁶¹ Congress did not impose a variable legal standard that fluctuated with the capacity of the vessels or the amount of cargo they were carrying. Under the statute, customs had the same authority to search an East Indiaman⁶² as a dinghy, and as far as we can tell both inspections proceeded under the same

⁵⁷ 431 U.S. 606, 619-20 (1977).

⁵⁸ 541 U.S. 149, 154-55 (2004).

⁵⁹ See generally *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution, Civil Rights and Property Rights of the S. Comm. on the Judiciary*, 110th Cong. (2008) (statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation).

⁶⁰ Alzahabi, *supra* note 16, at 179-80; see also Christine A. Coletta, Note, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971, 999 (2007) (“A person should have an expectation that the information on his computer . . . would be kept more private than a wallet or handbag, which also contain private items but have the capability and likelihood of storing much less.”).

⁶¹ Act of July 31, 1789, c. 5, § 24, 1 Stat. 29.

⁶² East India men were massive 18th century merchant vessels, typically measuring between 1100 and 1400 registered tons.

legal standard. If the 1789 customs statute is evidence – albeit maybe not conclusive evidence – that the Framers embraced something like the modern border-search doctrine, it might also stand for the proposition that the standard under which those searches may be conducted does not depend on the amount of material the container carries.

Nor is it accurate to say that the “massive container” problem posed by laptops is historically unprecedented. It’s certainly true that, with the ubiquity of laptop computers, more and more people are crossing international borders with large amounts of content in tow. But people have been entering the United States with massive containers for decades, maybe centuries, and the border-search doctrine has not applied differently to them. Laptops might have democratized the practice, but they did not create it. To see why this is so, consider two examples from the analog world: searches of large merchant vessels and moving trucks.

A typical container ship will carry anywhere from ___ to ___ containers, each of which is capable of transporting ___ cubic yards of cargo.⁶³ That’s a staggering ___ cubic yards of cargo per vessel. Yet these enormous ships historically have been searched under the same suspicionless standard that governs all other routine border inspections. A modern descendent of the 1789 act authorizes customs officers, “at *any* time,” to board “*any* vessel” and search “*every* part thereof,” as well as “*any* person, trunk, package, or cargo on board” – all without particularized suspicion.⁶⁴ In 2007, Congress mandated that every U.S.-bound container must be physically inspected for security threats (including through x-ray and radiation scans) before setting sail for this country, again without any particularized suspicion.⁶⁵ Seafaring vessels have grown larger and larger over the years, and searches of them have grown more and more comprehensive, but the border-search doctrine has remained constant. It has not been adjusted to require particularized suspicion due to the simple fact that ships are now capable of carrying more content. It is difficult to see why a similar adjustment should be made to accommodate laptop computers.

Moving trucks are another instructive example. People who relocate their households from Canada or Mexico to the United States cross the border laden with many of their possessions. Yet, despite the amount of material they carry, they are still subject to suspicionless border searches. In one recent case, the Fourth Circuit upheld a suspicionless border search of the defendant’s van even though the vehicle “appeared to contain ‘everything [he] own[ed].’”⁶⁶ Nowhere did the court suggest that the quantity of content was relevant to the question whether the search of the van should be deemed routine or non-routine.

Treating laptops differently because of the amount of data they contain is also unsound for policy reasons. A legal standard that fluctuates based on the container’s size would privilege those who cross the border with large amounts of content over those who carry small amounts. The level of privacy protection a traveler enjoys thus would hinge on a mere happenstance – how

⁶³ CITE.

⁶⁴ 19 U.S.C. § 1581(a) (emphases added).

⁶⁵ Cite 9/11 legislation.

⁶⁶ *United States v. Ickes*, 393 F.3d 501, 502 (4th Cir. 2005).

large his container is. People who travel with small containers (a tourist with a suitcase, a businessman with a briefcase) would receive only perfunctory protection under the Fourth Amendment. People who travel with large containers (a journalist carrying his laptop, the captain of a container ship) would receive more. Yet the amount of privacy an international traveler legitimately may expect at the border should not depend on something as arbitrary as the capacity of the container he is carrying.

This is why efforts to analogize laptop computers to homes are ultimately unpersuasive. Houses and laptops may well contain comparably massive volumes of material. Yet the reason the home enjoys uniquely robust privacy protections in the Anglo-American legal tradition is not because of how much it contains. (The Fourth Amendment protects a one-room shanty as much as it does a sprawling mansion.⁶⁷) The home occupies a privileged place 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 poorest man may in his cottage bid defiance to all the forces of the Crown.”⁶⁸ 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.”⁶⁹

Nature of information. Another obvious difference between laptops and other property is the type of content they store. A suitcase might contain shampoo and dirty socks, and a cargo container might be filled with tires. But computers often store data of extreme sensitivity. Laptop searches thus “could reveal much more personal information than what is found when customs officials pat down a passenger, . . . ask her to empty her pockets, or rifle through her luggage.”⁷⁰ On this view, laptops amount to “extensions of the self,” and searches of them “implicate[] dignity and privacy interests on par with physical intrusions.”⁷¹ All that is true, but the intensely personal nature of the data kept on computers still does not justify a special reasonable-suspicion requirement for laptop searches. Such a rule would violate the principle of technological neutrality.

Laptop searches are not unique in their ability to reveal sensitive personal information. Travelers might cross the border with letters, address books, photo albums, and similar items.

⁶⁷ Cf. *United States v. Ross*, 456 U.S. 798, 822 (1982) (emphasizing that the Fourth Amendment protects “a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf” to the same extent it protects a “sophisticated executive with [a] locked attaché case”).

⁶⁸ *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.”).

⁶⁹ *United States v. Thirty-seven Photographs*, 402 U.S. 363, 376 (1971).

⁷⁰ Coletta, *supra* note 51, at 1001; see also Alzahabi, *supra* note 16, at 179 (“[A] laptop search could reveal just as much private information about a person as a strip search or other intrusive body search can.”).

⁷¹ John W. Nelson, Note, *Border Confidential: Why Searches of Laptop Computers at the Border Should Require Reasonable Suspicion*, 31 AM. J. TRIAL ADVOCACY 137, 141 (2007).

Yet even though each of these objects can contain personal information of great sensitivity, courts generally permit customs officers to search them at the border without any individualized suspicion.⁷² It's hard to see why data that is stored electronically should be entitled to stronger privacy protections than the very same data would be if stored physically. A laptop computer is essentially an electronic suitcase; it's a correspondence file, address book, and photo album, digitized and stored in a single container. A special carve-out from the ordinary rules governing routine border searches would mean that the level of protection for messages, contacts, photos, and other data would vary based on whether they are kept in digital or analog format. The amount of privacy travelers enjoy in their personal information would not depend on the nature of the data itself. It would turn on the happenstance of whether that data is reproduced with ink and paper or with ones and zeros.⁷³ Such a rule would privilege the tech-savvy and undervalue the privacy interests of Luddites. The better course is to retain a uniform legal standard that applies regardless of the medium in which the information happens to be stored.

Indeed, the Supreme Court has stressed that the rationales underlying the border-search doctrine – not transactional fortuities – are what should determine the magnitude of travelers' privacy rights at the border. *Ramsey v. United States* upheld the power of customs officers to open inbound international mail in search of contraband. The Court emphasized 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.”⁷⁴ 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.⁷⁵

Of course, searches of correspondence and other expressive materials stored on laptops raise special concerns that might make it appropriate to adjust the border-search doctrine; such inspections “reflect a convergence of First and Fourth Amendment values.”⁷⁶ Several courts have denied that the border-search doctrine applies any differently to expressive content than it does to other materials.⁷⁷ But the jury is still out. After all, the Supreme Court in *Ramsey* found

⁷² See, e.g., *United States v. Seljan*, 497 F.3d 1035, 1041 (9th Cir. 2007) (letters), *reh'g en banc granted*, 512 F.3d 1203 (9th Cir. 2008); *United States v. Soto-Teran*, 44 F. Supp. 2d 185, 191-92 (E.D.N.Y. 1996) (address books), *aff'd*, 159 F.3d 1349 (2d Cir. 1998); *United States v. Ickes*, 393 F.3d 501, 503 (4th Cir. 2005) (photo albums).

⁷³ See Kerr, *supra* note 7, at 538-39 (“Every letter, number, or symbol is understood by the computer as a string of eight zeros and ones. For example, the upper-case letter ‘M’ is stored by a computer as ‘01001101,’ and the number ‘6’ as ‘00110110.’”).

⁷⁴ *United States v. Ramsey*, 431 U.S. 606, 620 (1977).

⁷⁵ 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.”).

⁷⁶ *United States v. United States District Court*, 407 U.S. 297, __ (1972) (“*Keith*”).

⁷⁷ See, e.g., *Tabbaa v. Chertoff*, 509 F.3d 89, 102 n.5 (2d Cir. 2007) (“It may also be true that the First Amendment's balance of interests is qualitatively different where, as here, the action being challenged is the government's attempt

it “unnecessary to consider” whether searches of incoming international mail violated the First Amendment; part of the reason it stayed its hand was that, under the governing statute, “[e]nvelopes are opened at the border only when the customs officers have reason to believe they contain other than correspondence, while the reading of any correspondence inside the envelopes is forbidden” by regulation.⁷⁸ If border officials were opening envelopes and reading letters without reasonable suspicion, the *Ramsey* Court might have been less willing to uphold their authority.⁷⁹

The problem of reconciling the First Amendment and the border-search doctrine is not unique to laptop searches. Concerns about inspections of expressive materials are present regardless of whether customs is examining snail-mail or email. It would take us well beyond the limited scope of this article to consider whether these inspections ought to be governed by something more than the lax standard for routine border searches. For our purposes, it is enough to call for technological neutrality here as well. Whatever the standard may be, rigorous or relaxed, it should apply equally to searches of analog media as it does to searches of digital media.

Retention of information. A third and final difference between laptop searches and their traditional analog counterparts has to do with the manner in which digital inspections are carried out. Searches of luggage and other physical goods are self-contained transactions. Once the search is complete, the traveler goes about his business, and the government retains none of his property (unless, of course, the inspection uncovers contraband or evidence of crime). By contrast, the government often conducts a laptop search by copying the entirety of the computer’s hard drive, and investigators retain the data for future analysis. The potential thus exists for a laptop search to entail lengthy, and maybe even permanent, possession of the data by the government. In short, laptop inspections can muddy the distinction between searches and seizures. While the previous two differences do not, in my view, justify abandoning the ordinary Fourth Amendment rules for border searches of laptops, this unique feature of computer inspections does warrant special protections above and beyond the ones that apply in the analog world.

to exercise its broad authority to control who and what enters the country.”); *Seljan*, 497 F.3d at ___ (___); *United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005) (refusing to “recognize[e] a First Amendment exception to the border search doctrine”).

⁷⁸ *Ramsey*, 431 U.S. at 624 (citing 19 U.S.C. § 482; 19 C.F.R. § 145.3). To complicate matters even further, there are a number of potentially overlapping statutes that govern searches of incoming and outgoing letters. 19 U.S.C. § 482(a) – the statute at issue in *Ramsey* – provides that customs officers may not inspect an “envelope” unless they have “reasonable cause to believe [it] is subject to duty, or to have been unlawfully introduced into the United States.” 19 U.S.C. § 1583 likewise requires customs to have reasonable suspicion to open sealed outbound envelopes carried by the U.S. Postal Service. On the other hand, 31 U.S.C. § 5317(b) broadly authorizes suspicionless searches of “any envelope or other container . . . entering or departing from the United States,” for purposes of enforcing federal currency reporting requirements. Some courts have held that Section 5317 grants “separate and independent authority” to search letters without suspicion, effectively rendering Section 482 and Section 1583 “irrelevant.” *Seljan*, 497 F.3d at 1041.

⁷⁹ *Cf. Seljan*, 497 F.3d at 1048, 1049 (Pregerson, J., concurring in part and dissenting in part) (arguing that, because “allowing government officials to read private papers without individualized suspicion risks serious intrusions on privacy,” the government “must have reasonable suspicion that papers in a package constitute contraband or evidence or wrongdoing before officers may read the contents of those papers”).

Computer searches typically begin with officers making an exact, complete copy of all the data contained on the hard drive or other storage device they wish to inspect. Professor Orin Kerr emphasizes that, “[i]n most computer search cases, government investigators create a bitstream copy of the storage device and then search the image rather than the original.”⁸⁰ A bitstream copy “duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original.”⁸¹ Customs officers then will search the data they have mirrored, instead of the original data on the traveler’s laptop. Digital searches thus are very different from analog ones. “In the world of physical evidence, the police generally need to take evidence away to obtain it. The definition of seizure is tied to the taking. In contrast, computer data is nonrivalrous: investigators can obtain a perfect copy without depriving the owner of the original.”⁸² Because there is no need to return the bitstream copy to the owner – the owner has had the original data in his possession all along – the government presumably could retain it for extended periods of time once the analysis is complete, perhaps perpetually.

Commentators dispute how much legal significance should attach to the fact that searches of computers often involve mirroring a hard drive. Lee Tien argues that merely copying a hard drive, without more, is a seizure. When the government creates a perfect duplicate of a traveler’s data, it interferes with his possessory interests in that information. Copying data eliminates the owner’s right to exclude others, and for that reason copying amounts to a seizure of the data.⁸³ By contrast, Professor Kerr maintains that the simple act of copying data from a hard drive is neither a search nor a seizure of that data – although he acknowledges that commandeering a computer for the period of time necessary to copy the hard drive does amount to a seizure of the computer⁸⁴ (though perhaps not of the data it contains). For Professor Kerr, a search takes place only when the “data is exposed to human observation, such as through a computer monitor.”⁸⁵

This article does not engage the larger issue of the point at which government manipulation of digital data becomes a search or seizure within the meaning of the Fourth Amendment. That question is hugely significant in ordinary criminal investigations but it has less importance at the border, where customs officials are allowed to conduct many types of Fourth Amendment searches without warrant, probable cause, or even reasonable suspicion. Still, the prospect that officers might retain laptop data even after they have analyzed it and found nothing suspicious raises special concerns, and these special concerns justify special protections that might not be necessary in the case of traditional border searches. I discuss some possible additional safeguards below in Part IV.

⁸⁰ Kerr, *supra* note 7, at 557.

⁸¹ *Id.* at 541.

⁸² *Id.* at 560.

⁸³ *See* Tien, *supra* note 59, at __.

⁸⁴ *See* Kerr, *supra* note 7, at 561 (“Because imaging generally requires commandeering the computer and disabling access to the computer for a matter of hours, the computer ordinarily is ‘seized’ during this time under the existing definition of ‘seizure.’” (footnotes omitted)).

⁸⁵ *Id.* at 535.

C. *Intrusiveness Reconsidered*

The conventional wisdom is that border inspections of laptop computers are an especially intrusive kind of search, maybe even rivaling the invasiveness of a strip or body-cavity search.⁸⁶ Yet, somewhat counterintuitively, laptop searches have the potential to be *less*, not more, intrusive than traditional border searches of luggage and cargo. In a standard border search, customs officers must manually rifle through travelers' belongings, personally inspecting every item to determine whether it is contraband or evidence of crime. But if officers search a laptop by conducting a basic keyword search, an automated and impersonal computer process will be responsible for finding the investigative needles in the haystack – i.e., separating the small pieces of data that might have investigative significance from the larger mass of information that has no relevance to the government's counterterrorism or law-enforcement functions. As a result, officers may not need to screen personally the great mass of information stored on a traveler's laptop. They will only encounter discrete pieces of data that are flagged in the keyword search.

To see how laptop searches can be less intrusive than traditional border searches, compare the following two examples. A customs officer wants to see whether an arriving traveler knows anyone who has used the same cell-phone number as Mohamed Atta, the operational leader of the 9/11 hijackers.⁸⁷ (This sort of link analysis can be a helpful way of uncovering hidden ties between known terrorists and their unknown associates. According to a Markle Foundation report, rudimentary link analysis – comparing phone numbers, addresses, frequent-flyer numbers, and the like – would have enabled counterterrorism investigators to identify all 19 of the September 11 hijackers before the attacks.⁸⁸) The officer asks the traveler to hand over his address book. He then thumbs through the pages, reviewing each entry to see if it includes Atta's phone number. In the process, the details of the traveler's complete social network are displayed to the officer; the officer (if he is paying attention) can develop a fairly comprehensive understanding of the personal, professional, political, and religious circles in which the traveler moves. This exposure to the traveler's social network is not the intended goal of the search; the officer doesn't care who his friends are, he only cares whether he has ties to Mohamed Atta. But exposure is an inevitable byproduct of data searches in which a human being is responsible for initially scanning a data set to see if it contains anything that might merit further investigation.

Now consider what the inspection would look like if the traveler stores his contacts, not in a bound address book, but electronically in Microsoft Outlook. The customs officer asks the traveler to hand over his laptop. He then searches for Atta's phone number by keying a simple search string and running it against the contact data. (The officer might run the search directly on the traveler's laptop, perhaps by using Outlook's internal search function or by using stand-alone search software like Google Desktop. Or he might port the data to a customs computer and

⁸⁶ See, e.g., Kerr, *supra* note 7, at 569 (“[C]omputer searches tend to be unusually invasive. . . . Computer searches lower the cost and inconvenience of invasive searches, making such searches the norm rather than the exception.”).

⁸⁷ See 9/11 COMMISSION REPORT, *supra* note 8, at ___.

⁸⁸ See PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE: A REPORT OF THE MARKLE FOUNDATION TASK FORCE 28 (2002).

analyze it there.⁸⁹) It's no longer necessary for the officer personally to review each and every one of the traveler's contacts. The search engine will do it for him, and will only return a hit if one of the contacts includes Atta's phone number. The officer is not exposed to the bulk data that would enable him to draw a comprehensive picture of the traveler's social network. That unintended byproduct of the search no longer materializes, and officer only sees data that is possibly suggestive of ties to terrorists.

Keyword searches of laptop computers thus potentially enable officers to identify contraband and evidence in a way that imposes relatively weaker burdens on travelers. Not only can digital inspections promote efficiency (keyword searches might take less time than manually inspecting thousands of individual files⁹⁰), they also can protect travelers' privacy interests. Customs officers are not responsible for personally separating the wheat from the chaff; they do not identify and isolate the individual data points that might warrant further investigation from the mass of information that has no investigative value. A computer does that for them. Officers therefore need not encounter the raw data on travelers' laptops. It would be possible to restrict them to only those distinct pieces of data flagged by a computer as possibly indicating the presence of contraband or evidence of other crimes.

It might be helpful to think of a keyword search as a digital equivalent of a dog sniff. With dog sniffs, customs officers need not open each incoming suitcase to manually inspect it for illegal drugs. Instead, specially trained drug-sniffing dogs screen the baggage unopened. Officers then take a closer look at any suitcases as to which the dogs have alerted, signaling the possible presence of narcotics. Because dog sniffs eliminate the need for officers to manually inspect contents that may turn out to be innocuous, the Supreme Court has recognized that they represent less of an affront to travelers' privacy interests than traditional border inspections:

A "canine sniff" by a well-trained narcotics detection dog . . . does not require opening the luggage. It does not expose contraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage. Thus, the manner in which information is obtained through this investigative technique is much less intrusive than a typical search.⁹¹

The same can be true of laptop searches. Just as dog sniffs help customs detect narcotics without rifling through the entire contents of a suitcase, keyword searches of laptops likewise enable border officials to hunt for telltale signs of terrorism and child predation without meandering through massive volumes of sensitive personal data.

The potential privacy gains of digital searches could be especially significant in situations where border officials want to inspect travelers' correspondence, personal diaries, or other

⁸⁹ See Kerr, *supra* note 7, at 540 (indicating that a search of computer data typically "occurs on the government's computer, not the defendant's").

⁹⁰ *But see id.* at 543 ("Computer searches tend to require fewer people but more time. . . . [A]nalysis of a computer hard drive takes as much time as the analyst has to give it.").

⁹¹ *United States v. Place*, 462 U.S. 696, ___ (1983).

expressive materials. Keyword searches can reduce or even eliminate the need for officers to scan hundreds of stored emails between a business traveler and her husband, or between the imam of a mosque and its membership director, in search of a stray reference to Osama bin Laden. That kind of invasive inspection can be avoided by keying a simple search string – “Osama,” “al Qaeda,” “mujahedeen,” or “jihad” – and examining the results to see if further investigation of the traveler might be warranted. Not only can digital searches help promote travelers’ interest in personal privacy, they can help vindicate their free-speech interests. The availability of narrowly focused digital searches thus may reduce the number of instances in which travelers are put to a Hobson’s choice of curtailing their international travel or curtailing their constitutionally protected expressive activities.

At the same time, we should not overstate the privacy benefits of digital searches. My argument is not that laptops searches are inevitably less intrusive than traditional border inspections, it’s that they have the potential to be. There is no guarantee that customs officers will limit themselves to keyword-search techniques. Whether because of agency policy or in spite of it, they may choose to supplement a keyword search by rummaging through a traveler’s hard drive, thereby defeating any potential privacy gains. Similarly, even if a keyword search goes off without a hitch, at some point a human being will have to be exposed to the data the computer has flagged for potential follow-up. Customs officers may see less sensitive personal information than they otherwise would, but they will still see plenty. In addition, while digital searches have the potential to work well when customs is looking for text files (e.g., correspondence or contacts), they could be less effective in searches of graphic or video files (e.g., images of Osama bin Laden or video clips of child pornography) that might not be keyword-searchable. Customs officers may find it necessary to inspect those kinds of files manually.⁹²

Perhaps the most important qualification is this: The fact that a keyword search returns a hit is not a conclusive indication (and may not even be an especially probative indication) that the traveler is involved with terrorism, child exploitation, or any other crime. There might be entirely innocent explanations for a laptop with documents that mention “al Qaeda” and “jihad” – for example, the owner may be a journalist who covers the Middle East, or she may be a Muslim activist who works to combat extremism and promote understanding among people of different faiths. In other words, keyword searches are likely to return a number of false positives. (The same problem can arise with dog sniffs. A poorly trained or unreliable dog might alert in front of a suitcase that, when searched, is found to contain no contraband.) This is an important shortcoming, but not a fatal one. Even accounting for false positives, a focused keyword search of a laptop has the potential to do less violence to the owner’s privacy interests than a traditional wide-ranging search where officers manually inspect every item in her suitcase.

IV. ADDITIONAL PROTECTIONS: COLLECTION LIMITS VS. USE LIMITS

The Fourth Amendment imposes relatively weak constraints on the ability of customs officers to perform laptop searches at the border, but the Constitution is not the only source of

⁹² Professor Kerr observes that the National Drug Intelligence Center has compiled digital signatures for many known images of child pornography. *See* Kerr, *supra* note 7, at 546. It may be possible to check travelers’ laptops for signs of these digital signatures in a way that is similar to keyword searches.

privacy protections. Policymakers at the Department of Homeland Security or in Congress might consider implementing additional safeguards that go beyond what the Fourth Amendment demands. The need for supplemental protections is especially acute given the manner in which officials often perform laptop searches – i.e., by creating a bitstream copy of a traveler’s hard drive, which the government then can inspect at its discretion. What form should these additional safeguards take? Laptop searches may be an instance where the most appropriate way to balance travelers’ legitimate privacy and speech interests against the government’s counterterrorism and law-enforcement needs is not by limiting officers’ ability to gather information in the first place, but by restricting what they may do with the information they do gather. In short, we might prefer “use limits” over “collection limits.”⁹³

Collection limits seek to vindicate privacy interests in a fairly direct way: by restricting the circumstances in which the government lawfully may acquire certain data (and sometimes by prohibiting the government from collecting it at all). Collection limits are easy to come by. The preeminent example, of course, is the Fourth Amendment itself, which specifies that the government ordinarily may not conduct a search unless it establishes probable cause and obtains a judicial warrant.⁹⁴ The U.S. Code offers plenty of other examples. The Foreign Intelligence Surveillance Act generally bars the government from engaging in electronic surveillance unless it demonstrates, among other things, probable cause to believe that the target is a “foreign power” (e.g., a foreign government or terrorist organization) or an “agent of a foreign power” (e.g., a spy or terrorist).⁹⁵ Similarly, the government may not issue National Security Letters – a type of administrative subpoena used to obtain documents, like bank records and credit reports – unless those materials are relevant to (or sometimes necessary to) an espionage or terrorism investigation.⁹⁶

While collection limits are the traditional legal instrument for safeguarding privacy interests, use limits offer more indirect types of privacy protections. Use limits do not prevent the government from gathering information. The way they seek to promote privacy is by limiting what the government may do with the data it does collect (such as by restricting the sharing of information, or by allowing it to be employed only for specified purposes). One example is the Privacy Act, which bars federal agencies from disclosing “records” – i.e., information about a person, such as financial transactions and criminal records – unless various different exceptions apply.⁹⁷ Federal Rule of Criminal Procedure 6(e) likewise generally

⁹³ Cf. BENJAMIN WITTES, *LAW AND THE LONG WAR* 224 (2008) (arguing that “government should have relatively easy access to telecommunications and other data, the mining of which has an essential role to play in combating terrorism and other transnational threats,” but also calling for “stricter rules of – and accountability for – the use of that material, a punishing regime of retroactive accountability for misuse of data and violation of the rules”).

⁹⁴ See, e.g., *Katz v. United States*, 389 U.S. 347, 357 (1967).

⁹⁵ See 50 U.S.C. § 1805(a)(3)(A).

⁹⁶ See, e.g., 12 U.S.C. § 3414(a)(5)(A) (government may obtain financial records by certifying that they “are sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities”); 15 U.S.C. § 1681v(a) (government may obtain consumer credit reports by certifying that they are “necessary for the agency’s conduct or such investigation”). For a summary of the National Security Letter statutes, see generally Sales, *supra* note 18, at 849-53.

⁹⁷ See 5 U.S.C. § 552a(b).

prevents government lawyers and others from “disclos[ing] a matter occurring before the grand jury.”⁹⁸ The exclusionary rule also might be thought of as a use limit. While the exclusionary rule prohibits the government from introducing at trial evidence obtained in violation of the Fourth Amendment,⁹⁹ it permits the same information to be used for other purposes – e.g., the government may introduce it before a grand jury,¹⁰⁰ in deportation proceedings,¹⁰¹ in habeas corpus proceedings,¹⁰² and in other settings.

Use limits might be the best choice for regulating border searches of laptop computers, for a familiar reason. Special collection limits for laptops would violate the principle of technological neutrality. If policymakers enacted a statute or regulation that made it more difficult to search laptops than other types of property, the amount of privacy a traveler would enjoy in her personal information would depend on the medium in which she keeps it. Do you store your data on paper? The government can search with no suspicion at all. Do you store it electronically? The government can’t search unless it has reasonable suspicion. Privacy rights should not be determined by mere fortuities like these. Instead, use limits are capable of offering some protection to travelers’ privacy interests without the need to draw arbitrary lines between digital and analog media.

What specific safeguards should policymakers adopt? As a matter of first principles, Homeland Security should provide the public with as much information about the laptop searches it conducts 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.”¹⁰³ Transparency would help ensure that any abuses of customs’ laptop-search powers are corrected, and thus contribute to the searches’ perceived legitimacy. In particular, the government should reveal the number of laptop inspections it conducts each year, so citizens can judge the magnitude of the problem for themselves. Certain operational details may need to be kept under wraps to prevent the government’s intelligence sources and methods from being compromised.¹⁰⁴ In those cases, officials could provide classified briefings to the appropriate Members of Congress in lieu of full public disclosure.

The government has begun to make some of this information public, albeit in a piecemeal way. On the numbers front, Homeland Security has indicated that 40 of the 17 million people

⁹⁸ Fed. R. Crim. P. 6(e).

⁹⁹ See *Weeks v. United States*, 232 U.S. 383, ___ (1914) (holding that “in a federal prosecution the Fourth Amendment barred the use of evidence secured through an illegal search and seizure”); see also *Mapp v. Ohio*, 367 U.S. 643, ___ (1961) (applying exclusionary rule to states).

¹⁰⁰ See *United States v. Calandra*, 414 U.S. 338, ___ (1974).

¹⁰¹ See *INS v. Lopez-Mendoza*, 468 U.S. 1032, ___ (1984).

¹⁰² See *Stone v. Powell*, 428 U.S. 465, ___ (1976).

¹⁰³ Sales, *supra* note 18, at 816.

¹⁰⁴ 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))).

who entered the United States from August 1 to 13, 2008 had their laptops inspected.¹⁰⁵ That’s roughly equal to about 960 laptop searches per year. The agency also has released a short document entitled “Policy Regarding Border Search of Information.”¹⁰⁶ That document sets forth rules that explain what types of electronic media may be searched, the circumstances in which data may be copied and retained, safeguards for handling especially sensitive types of information, and other standards. It’s a good start, but a four-and-a-half-page policy statement lacks the detail and authority associated with other types of administrative publications. Agency policymakers would do well to elaborate in a Privacy Impact Assessment¹⁰⁷ or a similar notice in the Federal Register.

Second, the government 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? Their criminal records? The manner in which they paid for their airline tickets? Tips from other government agencies about particular passengers? 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, the government may have good reasons to stop short of fully disclosing 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.¹⁰⁸

Third, policymakers should establish protocols for resolving the false positives that inevitably will result when customs officers run keyword searches against digital data. What procedures will the government use to tell which hits might indicate terrorism or other criminal activity, and which are innocuous? Policymakers should make clear that, because of the risk of false positives, a laptop search should not be the only factor used to determine whether a particular traveler represents a threat. Customs officers should take into account other evidence that the passenger may or may not be up to no good, such as his personal demeanor, record of past criminal convictions, and so on. And it goes without saying that travelers should be given the opportunity to explain that the suspicious material on their laptops is actually there for innocent reasons – e.g., the Middle East correspondent with documents that mention al Qaeda and jihad.

Fourth, 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

¹⁰⁵ See letter from Donald Kent Jr., Assistant Secretary for Legislative Affairs, U.S. Dep’t of Homeland Security, to Sen. Russ Feingold, Sept. __, 2008, cited in Josh Gerstein, *Feingold Bill Would Limit Searches of Travelers’ Laptops*, N.Y. SUN, Sept. 30, 2008.

¹⁰⁶ http://www.cbp.gov/linkhandler/cgov/travel/admissability/search_authority.ctt/search_authority.pdf

¹⁰⁷ See E-Government Act of 2002, § 208, Pub. L. No. 107-347, __ Stat. __, __ (2002) (codified at __ U.S.C. § __) (directing federal agencies to conduct Privacy Impact Assessments before gathering personal information that “will be collected, maintained, or disseminated using information technology”).

¹⁰⁸ 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.”).

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, 90 minutes if done on-site at the airport, or within 48 hours if the laptop is taken to an off-site computer forensics facility. But at a minimum, customs could set goals to encourage effective yet speedy searches. Unfortunately, the DHS policy statement doesn't do much in this regard. It merely recites the boilerplate goal that laptop searches should be completed within "a reasonable period of time."¹⁰⁹

The government also ought to adopt standards on the retention and use of data gathered from laptop searches. If an inspection fails to uncover any criminal activity, customs 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. In this vein, the Homeland Security policy statement properly directs officers to destroy any data they have copied "if after reviewing the information there is not probable cause to seize it."¹¹⁰ In other words, while officers may conduct a laptop search without individualized suspicion, they may not keep any data unless they can meet the exacting probable-cause standard.¹¹¹ (The policy does not, however, appear to require them to obtain a judicial warrant before retaining the data.)

Sixth, in addition to these generally applicable data-retention and –use standards, the government should adopt special rules governing access to especially sensitive types of information. Customs 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. Again, the DHS policy statement represents a good first step. Homeland Security's policy statement helpfully directs officers to "take all reasonable measures to protect" business or commercial information "from unauthorized disclosure." And it makes reference to the Trade Secrets Act and Privacy Act, both of which impose penalties on government employees who disclose certain types of private information.¹¹² But because the policy statement doesn't offer any guidance on which protective measures count as reasonable and which do not, it's not likely to offer much concrete protection. Somewhat more specifically, the policy statement flatly bars officers from searching materials "covered by attorney-client privilege" unless they first seek "advice" from customs lawyers or the local U.S. Attorney's

¹⁰⁹ Policy statement § (C)(1).

¹¹⁰ *Id.* § (C)(1); *see also id.* § (D)(1).

¹¹¹ The probable-cause requirement is comforting, but an exception threatens to swallow the rule. The policy statement authorizes officers to share copies of laptop data with other agencies when necessary to translate or decrypt it. *See id.* § (C)(2)(b). There is no requirement that other agencies must discard the information if they lack probable cause to seize it; instead, they may retain the data on their own "independent legal authority" if "the information is of national security or intelligence value." *Id.* § (D)(2)(c). Hence if customs officers ask CIA to decrypt data from a traveler's laptop, CIA may be able to keep the information even if further analysis reveals no criminal wrongdoing.

¹¹² *Id.* § (E)(1).

office.¹¹³ (Customs officers need not obtain their authorization; they apparently remain free to disregard the lawyers’ advice not to search privileged materials.)

Finally, Homeland Security 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.”¹¹⁴ It would have the same beneficial effect for laptop searches.

CONCLUSION

The problems posed by border searches of laptop computers aren’t going away anytime soon. Terrorists will continue to use laptops to plot their atrocities, and child predators will do the same to satisfy their twisted desires. Yet laptops themselves are morally neutral; they are as capable of being put to innocuous uses as insidious ones. As ever more law-abiding travelers cart their computers with them when they venture abroad, and as their capacity to store massive amounts of sensitive personal information continues to grow, it becomes increasingly important to set clear standards governing when customs officers may inspect laptops at the border and what they may do with the data they find.

The Fourth Amendment is a poor vehicle for establishing those rules. For many decades, the Supreme Court has held that border inspections of suitcases, packages, and other types of property – i.e., routine border searches – need not be justified by any individualized suspicion at all. These searches are deemed *per se* reasonable within the meaning of the Fourth Amendment simply because they occur at the border. Of course, laptops differ from other kinds of property in a number of significant ways. They contain more material, the data they store is intensely private, and digital searches can leave a permanent copy of the data in the government’s hands. While those differences are important, they do not, in general, justify a special judicial carve-out from the border-search doctrine.

Instead, the best hope for crafting standards that adequately balance the government’s needs and those of innocent international travelers lies with policymakers in Congress and the Executive Branch. Rather than imposing special collection limits that would restrict the government’s ability to inspect laptop computers (and that would violate the principle of technological neutrality), policymakers should insist on more robust use limits that regulate how government officials access, share, and otherwise employ the data they do extract from laptops. Those standards would equip the government with the tools it needs to protect its citizens and fight child exploitation, while helping to ensure that the privacy interests of law-abiding businessmen, journalists, and tourists don’t become collateral damage in the war on terrorism.

¹¹³ *Id.* § (E)(3).

¹¹⁴ *United States v. Flores-Montano*, 541 U.S. 149, 156 (2004) (Breyer, J., concurring) (citation omitted)