3-1-2009

Run for the Border: Laptop Searches and the Fourth Amendment

Nathan Alexander Sales
George Mason University School of Law

Follow this and additional works at: https://scholarship.richmond.edu/lawreview

Part of the Constitutional Law Commons, Criminal Law Commons, Evidence Commons, Internet Law Commons, and the National Security Law Commons

Recommended Citation
Available at: https://scholarship.richmond.edu/lawreview/vol43/iss3/10

This Article is brought to you for free and open access by the Law School Journals at UR Scholarship Repository. It has been accepted for inclusion in University of Richmond Law Review by an authorized editor of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.
I. INTRODUCTION

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

U.S. Customs and Border Protection officers at Dallas-Fort Worth knew that Irving was a convicted pedophile and 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." While analyzing the disks, investigators discovered "[i]mages of child erotica." Five years later, a search of the computer in Irving’s Brooklyn apartment uncovered seventy-six video files of "prepubescent

* 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 Before the Subcomm. on the Constitution, Civil Rights and Property Rights of the S. Comm. on the Judiciary, 110th Cong (2008) (statement of Nathan A. Sales, Assistant Professor of Law, George Mason University School of Law), http://www.law.gmu.edu/assets/files/news/Laptop_search_testimony(06232008).pdf. Thanks to Larry Cunningham, Orin Kerr, Mike O’Neill, Jeremy Rabkin, and Lee Tien for their helpful comments.

1. United States v. Irving, 452 F.3d 110, 114 (2d Cir. 2006).
2. See id.
3. See id. at 114–15.
4. Id. at 115.
5. Id.
6. Id.
boys engaging in various sexual acts with each other and in other cases of sexual acts by themselves.\textsuperscript{7}

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."\textsuperscript{8} Irving "preferred prepubescent boys, under the age of 11."\textsuperscript{9}

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.\textsuperscript{10} Society justifiably applauds the incapacitation of child predators. But the border search that helped secure Irving's conviction raises some vexing problems. When told that the government claims the power to rummage through travelers' laptops, BlackBerrys, and flash drives at the border, many people react with shock, even revulsion. A laptop search seems terribly invasive. The most intimate details of a person's life—e-mails to friends and colleagues, family photographs, financial records, and so on—are paraded in front of the officers 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 international borders. For instance, should customs officers at the Department of Homeland Security ("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 can establish reasonable suspicion, or perhaps even demonstrate probable cause and obtain a judicial warrant? Do searches of laptop computers present unique problems that aren't present when officers inspect suitcases, packages, and other types of property? If so, do those differences justify a different Fourth Amendment standard for laptop searches?

\textsuperscript{7} Id. at 115--16.
\textsuperscript{8} Id. at 114.
\textsuperscript{9} Id. at 115.
\textsuperscript{10} See id. at 114.
This article argues that suspicionless border searches of laptop computers generally are permissible under the Fourth Amendment. Part II examines the range of compelling, and often competing, interests 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’ interests in personal privacy and free expression.

Part III discusses the Supreme Court of the United States’s border search doctrine. According to the Court, “non-routine” border searches (invasive searches of the body, for example) are subject to the reasonable-suspicion standard, but “routine” searches (such as searches of property) need not be preceded by any individualized suspicion.11 In other words, routine searches satisfy the Fourth Amendment’s reasonableness requirement “simply by virtue of the fact that they occur at the border.”12

Part IV 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 is “routine”; customs officers therefore don’t need reasonable suspicion before inspecting a particular traveler’s computer.13 That’s probably the correct result for a simple reason: technological neutrality. The privacy protections travelers enjoy should not depend on whether they store their data in digital format or on paper. Customs officers can search address books and photo albums at the border with no suspicion at all, and the same rule should apply to travelers who keep their contacts and pictures on a laptop. It’s true that laptops are different from other types of property: They potentially contain much more data than other items that cross the border. And the information laptops do contain can be quite sensitive and revealing—for example, photo albums, e-mails, and records of the owner’s web browsing. In addition, customs officers might 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 those differences do not justify a blanket

11. See United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985); Irving, 452 F.3d at 123.
13. See infra notes 92–95 and accompanying text.
“laptop exception” to the border search doctrine. In fact, laptop inspections have the potential to be less intrusive than traditional border searches of physical objects. With laptop searches, automated and impersonal computer processes such as keyword queries can identify specific data points that might warrant further investigation. These processes may eliminate the need for customs officers to sift through the information manually.

Finally, Part V discusses legislative and 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 may want to implement other safeguards that supplement these relatively weak constitutional protections. 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 has modest aims. It does not comprehensively address government searches or seizures of data stored in electronic format. Rather, it focuses on one particular manifestation of that problem—electronic searches at the border. Similarly, it does not discuss customs officers’ power to inspect travelers’ laptops in connection with domestic flights; the article is limited to searches that occur at international borders. Lastly, this article does not mount an independent defense of the border search doctrine on originalist, normative, or other grounds. 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 this article poses is not “should we have a border search doctrine?”, but rather, “given that we have a border search doctrine, how should it apply to laptops?”

II. THE COMPETING INTERESTS OF LAPTOP SEARCHES

As is often the case in Fourth Amendment law, laptop searches pit strong governmental interests against the equally powerful interests of ordinary citizens. On the government’s side of the ledger, there is a paramount interest in incapacitating terrorists who may be trying to enter this country.15 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 inspection points.”16 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 passengers’ belongings, including their computers, when they land.

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 information about crop-dusting aircraft and wind patterns.17 If customs officers 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 Osama bin Laden’s terrorist network.18 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 customs officers could have used that information to identify other Al-Qaeda operatives in the United States. Still, it’s

18. 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 16, 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.”).
possible that a border search of Moussaoui's computer may have uncovered clues that could have shed some light on the 9/11 plot.

More recently, in 2006, a laptop search at Minneapolis-St. Paul airport helped Customs detect a potentially risky traveler.\footnote{See Remarks of Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Security, at the Ctr. for Strategic and Int'l Studies (Dec. 19, 2006), http://www.dhs.gov/xnews/speeches/sp_1166557969765.shtm (last visited Feb. 27, 2009).} Once he was referred to secondary inspection, officers discovered that he had a manual on making improvised explosive devices ("IEDs")—weapons of choice for terrorists in Afghanistan and Iraq.\footnote{See id.} 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."\footnote{See id.} Government officials have claimed other counterterrorism victories as well:

During border searches of lap tops [sic] customs 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 [the] U.S. and its citizens. These materials have led to the refusal [of] admission and the removal of these dangerous people from the United States.\footnote{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), http://rawstory.com/images/other/aherntestimony.pdf.}

This account is as regrettably short on details as it is painfully long on typos. Perhaps its brevity is due to government fears that publicity about national security operations might alert terrorists about 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. Still, it's not much of a stretch to say that laptop searches have the potential to reveal terrorist operatives, financiers, and handlers.

Terrorism is not the only threat laptop searches can detect. Suspicionless inspections of international travelers' computers have also proven instrumental in the government's efforts to combat child pornography and even ghastlier forms of child exploitation. To date, there have been twelve federal court decisions
examining the scope of the government’s authority to search laptops at the border, and every single one has involved child pornography.\textsuperscript{23} Unfortunately, Stefan Irving is far from an anomaly.\textsuperscript{24}

For instance, a 2000 search at the United States-Canada border uncovered a computer and some seventy-five disks containing child pornography.\textsuperscript{25} 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.”\textsuperscript{26} A 2006 border search of a vehicle at Bar Harbor, Maine likewise turned up a laptop with numerous images of child pornography.\textsuperscript{27} Agents also found “children’s stickers, children’s underwear, children’s towels or blankets with super heroes printed on them,” as well as twelve to fifteen condoms and “a container of personal lubricant.”\textsuperscript{28} And in 2007, a border search of an external hard drive at Del Rio, Texas, revealed “101,000 still images depicting child pornography” and “890 videos depicting pornographic images of children.”\textsuperscript{29}

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 e-mailing encrypted files to themselves. Then they could access the data after entering the country. It has been suggested that these alternative methods make laptop searches ineffective, and even constitutionally unreasonable.\textsuperscript{30} Yet the fact that terrorists and others might use a number

\begin{footnotesize}
\begin{enumerate}
\item See infra notes 92–95 and accompanying text.
\item See supra notes 1–10 and accompanying text.
\item United States v. Ickes, 393 F.3d 501, 502–03 (4th Cir. 2005).
\item Id.
\item Id. at *2.
\item United States v. McAuley, 563 F.2d 672, 675 (W.D. Tex. 2008).
\item 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), http://judiciary.senate.gov/pdf/08-06-25Peter_Swire_Testimony.pdf, at 12 (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,
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 swallowers in appropriate circumstances. Laptop searches may not be a perfectly effective way of interdicting contraband or detecting terrorist threats, but they do not 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. The need to prevent the departure of security threats might seem 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 uncover messages, contacts, and other data that reveal the identities of previously unknown associates. Or they might be leaving to attack outbound international flights, and a search at departure could help disrupt the plot.

Likewise, the removal of child pornography from this country might not seem to 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 to enforce laws against traveling abroad to engage in sexual acts with children, or as a quid pro quo to induce other countries to stem the flow of child pornography from their territories. Outbound laptop searches can also 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 inter-

Note, Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers, 41 IND. L. REV. 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.").
ests are at their zenith at the passport-control booth, but they aren't nonexistent at the departure gate.\textsuperscript{31}

While the government's interests 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' laptops 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."\textsuperscript{32} Privacy concerns are particularly acute when the traveler is a U.S. citizen, because courts generally recognize that Americans have stronger privacy interests under the Constitution than aliens who are only visiting this country temporarily.\textsuperscript{33}

Laptops can contain massive amounts of information. A modern-day 250-gigabyte hard drive is capable of storing the equiva-
lent of 125 million printed pages of text.\textsuperscript{34} It would only take sixty-three such devices to store the entire collection of the Library of Congress.\textsuperscript{35} Even a now-archaic eighty-gigabyte hard drive boasts an impressive storage capacity—the equivalent of forty million printed pages.\textsuperscript{36} That is equal to “the amount of information contained in the books on one floor of a typical academic library.”\textsuperscript{37}

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 e-mails sent and received over the course of years, and so on. A laptop can simultaneously function as a photo album, Rolodex, and correspondence file. In addition to personal data, business travelers may keep trade secrets and other proprietary information on their laptops. Physicians might store the medical records of hundreds of patients. Lawyers’ computers might contain 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 e-mail you have sent. It’s as if you’re crossing the border with your home in your suitcase.”\textsuperscript{38}

Border searches do not 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


\textsuperscript{35} Id.

\textsuperscript{36} Kerr, supra note 14, at 542.

\textsuperscript{37} Id.

crosses the border, he might be chilled from engaging in those activities in the first place. 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."

Searches of laptops can also place real strain on the right to travel. Business travelers and tourists might be reluctant to take to the skies if they fear that customs officers 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 cannot realistically minimize their expressive activities, such as journalists, opinion leaders, and activists, might cope with border searches by minimizing their overseas travel. People who cannot realistically minimize their overseas travel, such as global businessmen, might cope with border searches by minimizing their expressive activities. Either way, there is a risk that core constitutional values will be chilled.

III. THE SUPREME COURT'S BORDER SEARCH CASE LAW

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, the Supreme Court began to carve out an exception for border searches as early as 1886. In 1977, the

41. See, e.g., 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 Susan K. Gurley, Executive Director, Association of Corporate Travel Executives), http://judiciary.senate.gov/pdf/08-06-25Gurley_Testimony.pdf, at 11 (indicating that, in response to laptop searches, some "companies are purchasing additional computers that are scrubbed of any prior emails so that they can easily be replaced," and that some companies "senior executives are prohibited from carrying any computers" when they travel overseas).
43. See Boyd v. United States, 116 U.S. 616, 623 (1886); see also Carroll v. United
Court made it official. *United States v. Ramsey* held that "border searches were not subject to the warrant provisions of the Fourth Amendment and were 'reasonable' within the meaning of that Amendment."

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."45

There are two types of border searches: routine and non-routine. Routine searches—searches of cargo, luggage, and other property—"are not subject to any requirement of reasonable suspicion, probable cause, or warrant."46 For routine inspections, customs officers do not need any suspicion whatsoever, reasonable or otherwise.47 In other words, the Fourth Amendment permits customs officers to conduct "suspicionless" searches.48 This is not to suggest that the Fourth Amendment's reasonableness requirement does not apply at the border. It does.49 But routine border searches are deemed "reasonable simply by virtue of the fact that they occur at the border."50

Non-routine border searches are subject to the somewhat-more-exacting reasonable-suspicion standard. Before conducting a non-routine inspection, customs officers must have some particularized basis for suspecting that the person to be searched is en-

---

44. 431 U.S. 606, 617 (1977).
46. *See id.* at 538; *see also id.* at 551 (Brennan, J., dissenting) (agreeing that "thorough searches of [travelers'] belongings . . . do not violate the Fourth Amendment").
47. *Id.* at 538.
49. *Contra* Abramovsky, *supra* note 31, 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.").
50. United States v. Ramsey, 431 U.S. 606, 616 (1977). "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 619. "It is their entry into this country from without it that makes a resulting search 'reasonable.'" *Id.* at 620.
gaged in wrongdoing, such as carrying contraband.\textsuperscript{51} So what counts as a non-routine search? The Supreme Court has indicated that invasive searches of the body—including strip searches, body-cavity searches, and x-ray examinations—are non-routine.\textsuperscript{52} 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.”\textsuperscript{53} 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.\textsuperscript{54}

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.\textsuperscript{55} Customs officers tapped on the car’s gas tank and noticed it sounded solid.\textsuperscript{56} They called a mechanic, who removed the tank.\textsuperscript{57} When it was opened, investigators found about eighty pounds of marijuana.\textsuperscript{58} The Supreme Court unanimously upheld the inspection as a legitimate, routine border search.\textsuperscript{59} 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.\textsuperscript{60} 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.”\textsuperscript{61}

The second case, United States v. Montoya de Hernandez, is a particularly evocative example of a non-routine border inspec-
tion. Shortly after midnight, Rosa Elvira 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. 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, to which 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.” The next flight didn’t leave for a number of hours, and while the traveler initially agreed to the x-ray, she later withdrew her consent. She rejected option three for obvious reasons and eventually came to “exhibit[ ] symptoms of discomfort consistent with ‘heroic efforts to resist the usual calls of nature.’” Nature won. After more than 16 hours in custody, Montoya de Hernandez “passed 88 balloons containing a total of 528 grams of 80% pure cocaine hydrochloride.”

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, beyond the scope of a routine customs search and inspection,” is justified if customs officers “reasonably suspect that the traveler is smuggling contraband in her alimentary canal.” If the government wants to engage in non-routine border detention, it needs more particula-

63. Id. at 533.
64. Id.
65. Id. at 533–34.
66. Id. at 534.
67. Id. at 534–35.
68. See id.
69. Id. at 535 (quoting United States v. Montoya de Hernandez, 731 F.2d 1369, 1371 (9th Cir. 1984)).
70. Id. at 536–36.
71. See id. at 532, 544.
72. Id. at 541.
rized 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. 73 It bears emphasis that Montoya de Hernandez is a seizure case, not a search case. 74 Still, the ruling offers important insights into the Court’s understanding of what counts as non-routine. 75

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.” 76 By contrast, officials could search a “dwelling-house, store, building, or other place” only after obtaining a warrant. 77 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

73. See id. at 538, 541–43.
74. See id. at 544.
75. See id. at 541 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 United States v. Flores-Montano, 541 U.S. 149, 152 (2004).
76. Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43.
77. Id. 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.

Id.
as constitutionally permissible.\textsuperscript{78} This analysis has been nearly universally accepted by the judiciary.\textsuperscript{979}

The originalist defense is far from watertight. 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\textsuperscript{80}—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 officer may have a reason to suspect the presence of contraband that is constitutionally unreasonable—for example, a reason based on the race or ethnicity of the ship's captain. Scholars have pointed out additional flaws.\textsuperscript{81}

The Supreme Court has also grounded border searches in doctrinal and public-policy considerations. 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."\textsuperscript{82} The government likewise

\textsuperscript{78} See United States v. Ramsey, 431 U.S. 606, 616–19 (1977) (citing the 1789 statute to support the proposition that border searches are reasonable, without probable cause and without a warrant); Boyd v. United States, 116 U.S. 616, 623 (1886) (emphasizing that the 1789 act "was passed by the same Congress which 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).

\textsuperscript{79} Yale, \textit{supra} note 43, at 744.

\textsuperscript{80} Act of July 31, 1789, § 24, 1 Stat. at 43 (emphasis added).

\textsuperscript{81} For instance, Harris Yale emphasizes that the border search law was enacted before Congress considered the Bill of Rights: "Since 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, \textit{supra} note 43, at 746. Yale 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." \textit{Id.} at 739, 748; \textit{see also} Judith B. Ittig, \textit{The Rites of Passage: Border Searches and the Fourth Amendment}, 40 \textit{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"); \textit{Note, Border Searches and the Fourth Amendment}, 77 \textit{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").

\textsuperscript{82} United States v. Flores-Montano, 541 U.S. 149, 153 (2004); \textit{see also} Torres v. Puer-
has a "paramount interest" in keeping dangerous people and items on the other side of border. The magnitude of these governmental interests is reinforced by the diminished expectations of privacy held by international travelers: "[T]he expectation of privacy [is] less at the border than in the interior." At times, the Court stresses a legal theory of the arguably pre-constitutional origins of the government's search powers, other times it stresses the policy advantages that flow from embracing that theory. Thus, the two sets of considerations 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.

---

83. Flores-Montano, 541 U.S. at 155.
84. United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985); see also Cunningham, supra note 31, at 34–37. In some cases, the Court seems to suggest that privacy concerns are weaker at a border crossing because international travelers have no subjective expectation of privacy. See, e.g., Flores-Montano, 541 U.S. at 154 (indicating that "the expectation of privacy is less" partly because the Court's previous decisions put the public on notice "that automobiles seeking entry into this country may be searched"); United States v. Ramsey, 431 U.S. 606, 623 n.17 (1977) (explaining that "[t]here are limited justifiable expectations of privacy for incoming material crossing United States borders" in part because no statute creates such an expectation). Elsewhere the Court implies that privacy concerns are weaker because, even if travelers subjectively expect privacy at the border, society is not prepared to recognize that expectation as objectively reasonable. See, e.g., United States v. Ross, 456 U.S. 798, 823 (1982) ("The luggage carried by a traveler entering the country may be searched at random by a customs officer; the luggage may be searched no matter how great the traveler's desire to conceal the contents may be."). See generally Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (articulating a two-prong test for determining whether a "search" has occurred within the meaning of the Fourth Amendment: a subjective prong that considers whether persons have an actual expectation of privacy, and an objective prong that considers whether any such expectation is objectively reasonable).
86. See, e.g., Montoya de Hernandez, 473 U.S. at 541–42 (emphasizing the government's important interests in halting smuggling at the border).
87. See 3 WAYNE R. LAFAYE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10.5, at 325 (1978) (arguing that the Supreme Court has offered "a flimsy and not particularly satisfying explanation" of the border search doctrine); Yale, supra note 43, 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."); Note, supra...
IV. LAPTOP SEARCHES UNDER THE FOURTH AMENDMENT

As mentioned earlier, this article does not attempt to resolve whether or not the border search doctrine is sound. It is enough 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, or a non-routine search that must be justified by reasonable suspicion. The Supreme Court has never addressed the question. However, 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. In fact, laptop searches have the potential to be less intrusive than traditional border searches of travelers and their goods.

A. Laptops in Court

To date, twelve federal decisions have applied the Supreme Court's border search precedents to laptop computers and other electronic storage devices. Eight hold or imply that customs officers may search laptops at the border with no particularized suspicion: the Third Circuit, Fourth Circuit, Ninth Circuit (twice), District of Maine, Eastern District of Pennsylvania, Southern District of Texas, and Western District of Texas. Three courts—
the Second Circuit, Fifth Circuit, and District of Minnesota—dodged the question. The customs 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. Other than a single California district court that was reversed on appeal, 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 officers 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 has declined invitations to extend the more rigorous standards for invasive body searches into the realm of property searches on at least two prior occasions. In 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." Likewise, in Flores-Montano, the Court unanimously denied that border searches involving the disassembly of—and hence the potential for damage to—vehicles required reasonable suspicion. The Court appears to be drawing a rather bright-line rule: Invasive searches of the body might require reasonable suspicion, but

---

Tex. 2000), aff'd, 274 F.3d 1007, 1009 (5th Cir. 2001); cf. United States v. Romm, 455 F.3d 990, 997 n.11 (9th Cir. 2006) (reading Supreme Court case law 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).

91. See United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006); Roberts, 274 F.3d at 1012; United States v. Furukuwa, Crim. No. 06-145 (DSD/AJB), 2006 WL 3330726, at *1 (D. Minn. Nov. 16, 2006).

92. See Irving, 452 F.3d at 124; Roberts, 274 F.3d at 1012, 1016; Furukuwa, 2006 WL 3330726, at *1.

93. See United States v. Arnold, 454 F. Supp. 2d 999, 1000–01 (C.D. Cal. 2006), rev'd, 523 F.3d 941, 948 (9th Cir. 2008).


96. 541 U.S. at 154–55.
searches of property—even 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. First, laptops usually store vastly more content than a suitcase or a package of goods. Second, the material kept on a laptop will likely be more personal and sensitive than other types of property. Third, officers might search a laptop by mirroring its hard drive, which raises the possibility that the government could retain a permanent copy of the extracted data. Do any or all of these differences justify adopting a special rule for border searches of laptops? In general, no.

1. 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, such as a reasonable suspicion requirement. Yet, for history and policy reasons, it is inadvisable to distinguish among containers based on the amount of content they can carry. Size doesn't matter.


98. See id. at 5; 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, 999–1000 (2007).


100. See id. at 9.

101. See, e.g., Alzahabi, supra note 31, at 163, 179–80 (arguing for a reasonable suspicion standard because laptops "may contain an immense amount of information"); Coletta, supra note 98, at 999 ("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.").
First, consider history. The 1789 border search statute gave customs officials blanket authority to inspect "any vessel" that might contain goods subject to duty.\textsuperscript{102} 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, officials had the same authority to search an East Indiaman\textsuperscript{103} as a dinghy, and it appears that both inspections proceeded under the same legal standard.\textsuperscript{104} If the 1789 statute is evidence—albeit inconclusive evidence—that the Framers embraced something like the modern border search doctrine, the standard under which those searches may be conducted might 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 is certainly true that, with the ubiquity of laptop computers, increasingly more people are crossing international borders with large amounts of content in tow.\textsuperscript{105} 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.\textsuperscript{106} Laptops might have democratized the practice, but they did not create it. Consider two examples from the analog world: searches of large merchant vessels and moving trucks.

A typical container ship will carry anywhere from 5,000 to 11,000 twenty-foot-equivalent containers ("TEUs").\textsuperscript{107} A train carrying 11,000 TEUs would be forty-four miles long.\textsuperscript{108} That's a staggering amount of cargo per vessel. Yet these enormous ships historically have been searched under the same suspicionless standard that governs all other routine border inspections.\textsuperscript{109} A

\textsuperscript{102} Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43.

\textsuperscript{103} East Indiamen were massive 18th century merchant vessel ships, ranging between 400 and 1,500 registered tons. BRITANNICA ONLINE ENCYCLOPEDIA, East Indiaman, http://www.britannica.com/EBchecked/topic/176709/East-Indiaman.

\textsuperscript{104} § 24, 1 Stat. at 43; Coletta, supra note 98, at 983.

\textsuperscript{105} \textit{See Hearing, }Statement of Lee Tien, supra note 97, at 3.

\textsuperscript{106} \textit{See Alzahabi, supra note 30, at 167.}


\textsuperscript{108} \textit{Id.}

\textsuperscript{109} \textit{Cf.} United States v. Villamonte-Marquez, 462 U.S. 579, 585, 589 (1983) (holding that suspicionless boarding of vessels by government agents is "reasonable," because permanent checkpoints would not be practical on waters offering ready access to the open sea); United States v. Ramsey, 431 U.S. 606, 619 (1977) ("Border searches . . . have been
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"—without particularized suspicion. In 2007, Congress mandated that every U.S.-bound container must be physically inspected for security threats—including x-ray and radiation scans—before setting sail for this country, again without any particularized suspicion. Seafaring vessels have grown larger and larger over the years, and ship inspections have become progressively more comprehensive, but the border search doctrine has remained constant. It has not been adjusted to require particularized suspicion merely because 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 provide another instructive example. People who relocate their households from Canada or Mexico to the United States cross the border 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].''' Nowhere did the court suggest that the quantity of the cargo was relevant to 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. Thus, the level of privacy protection a traveler enjoys in an item would hinge on a mere happenstance—the size of the surrounding container. People who carry an object or

considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside.

110. 19 U.S.C. § 1581(a) (emphases added).
113. Cf. California v. Carney, 471 U.S. 386, 393 (1985) (refusing "[t]o distinguish between respondent's motor home and an ordinary sedan for purposes of the vehicle exception" to the warrant requirement because doing so "would require that [the Court] apply the exception depending upon the size of the vehicle and the quality of its appointments").
piece of information in a small container—a tourist with a suitcase or a businessman with a briefcase—would receive only perfunctory protection under the Fourth Amendment. People who carry that very same object or piece of information in a large container—a journalist carrying a laptop or the captain of a container ship—would receive more. In other words, the magnitude of a person's privacy interest in a photograph would depend on whether it is accompanied by many other items or only a few. The amount of privacy an international traveler legitimately may expect in an object should not depend on something as arbitrary as the capacity of the container in which it is carried.

Distinguishing among containers based on their sizes invites fairly obvious line-drawing problems. If we accept that a container's capacity should determine its owner's privacy expectations, the question becomes, how large must the container be to qualify for the special rule? These line-drawing problems could be particularly acute for electronic devices. In 2009, computers often ship from the factory with 250-gigabyte hard drives.114 In 2005, the typical hard drive held just eighty gigabytes.115 Is eighty gigabytes big enough to merit the massive-container treatment? Would it have been enough in 2005, when eighty gigabytes was considered state-of-the-art? Will it be in 2020, when an eighty-gigabyte hard drive will seem as archaic as a 5.25-inch floppy disk does today?116 More to the point, how would customs officers know the storage capacity of a hard drive—and hence whether the device qualifies as a massive container or a small one—unless they power it up and perform at least a cursory inspection? In other words, officers would have to conduct a suspicionless search to gain the information necessary to determine whether a suspicionless search is legally permissible. The better policy is to avoid these and other line-drawing difficulties and maintain a uniform rule for all containers, one that takes no notice of the containers' relative sizes.

The massive-container problem may explain why efforts to analogize laptop computers to homes are ultimately unpersuasive. Houses and laptops may well contain comparably large volumes

114. See Bellia, supra note 34, at 144.
115. See Kerr, supra note 14, at 542.
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 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.” Crossing an international border is in many ways the opposite of this kind of withdrawal. Rather than concealing himself from the government, a traveler voluntarily presents himself to the government for inspection and permission to enter the country. His expectation of privacy is considerably lower in those circumstances than when he is at his residence; “a port of entry is not a traveler’s home.”

2. 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. Computers, however, 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.” On this view, laptops amount to “extensions of the self,” and searching them “implicates dignity and privacy interests on par with physical intrusions.” All that is true, but the intensely personal nature of the data kept on computers still does not justi-

117. See United States v. Ross, 456 U.S. 798, 822 (1982) (emphasizing that “the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion,” and 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”).


119. 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”); Carter, 525 U.S. at 99 (“[I]t is beyond dispute that the home is entitled to special protection as the center of the private lives of our people.”).


121. Coletta, supra note 98, at 1000–01; see also Alzahabi, supra note 30, 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.”).

fy 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. Even though these objects can contain personal information of great sensitivity, courts generally permit customs officers to search them at the border without any individualized suspicion. It is hard to see why data stored electronically should be afforded stronger privacy protections than the same data would be if it were stored physically. A laptop is essentially an electronic suitcase; it is a correspondence file, address book, and photo album, digitized and stored in a single container. A special exception from the 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. Rather, it would turn on the happenstance of whether that data is reproduced with ink and paper or with ones and zeros. Such a rule would privilege the tech-savvy and undervalue the privacy interests of the 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 fortu-
ties, should determine the magnitude of travelers' privacy rights at the border. In Ramsey, the Court 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

124. See Kerr, supra note 14, 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.'").
126. Id. at 623–25.
[a letter's] mode of entry will be critical."\textsuperscript{127} 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."\textsuperscript{128} Just as the manner in which envelopes are transported is irrelevant to the privacy protections their owners enjoy, the scope of privacy at the border should not depend on whether 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.\textsuperscript{129}

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, like other national security operation, "reflect a convergence of First and Fourth Amendment values."\textsuperscript{130} Several courts have denied that the border search doctrine applies any differently to expressive content than it does to other materials.\textsuperscript{131} But the jury is still out. After all, the Supreme Court in Ramsey found it "unnecessary to consider" whether searches of incoming international mail violated the First Amendment.\textsuperscript{132} Part of the reason the Court stayed its hand was that, under the governing statute, "envelopes 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.\textsuperscript{133} If customs officers were

\textsuperscript{127} Id. at 620.
\textsuperscript{128} Id.
\textsuperscript{129} See United States v. McAuley, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008) ("The fact that a computer may take such personal information and digitize it does not alter the Court's analysis.").
\textsuperscript{131} See, e.g., Tabbaa v. Chertoff, 509 F.3d 89, 102–03 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 to exercise its broad authority to control who and what enters the country."); United States v. Seljan, 497 F.3d 1035, 1041–42 (9th Cir. 2007) ("[T]he government's justification for broad search authority is its interest in regulating the flow of persons and property across the border."); United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005) (refusing to "recogniz[e] a First Amendment exception to the border search doctrine").
\textsuperscript{132} Ramsey, 431 U.S. at 624.
\textsuperscript{133} Id. To complicate matters even further, there are a number of potentially overlapping statutes that govern searches of incoming and outgoing letters. The statute at issue
opening envelopes and reading letters without reasonable suspicion, the Ramsey Court might have been less willing to uphold their authority.\textsuperscript{134}

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 officers are examining snail mail or e-mail. It is 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. Rather, it is enough to call for technological neutrality. Whatever the standard may be, rigorous or relaxed, it should apply equally to searches of analog and digital media.

3. Retention of Information

A third and final difference between laptop searches and their traditional analog counterparts concerns 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 might search a laptop by copying the entire hard drive, with investigators retaining the data for future analysis.\textsuperscript{135} The potential thus exists for a search of a laptop to entail lengthy, and maybe even permanent, possession of data by the govern-

\textsuperscript{134} Cf. Seljan, 497 F.3d at 1048–49 (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 of wrongdoing before officers may read the contents of those papers").

\textsuperscript{135} See Kerr, supra note 14, at 557.
In short, inspections of laptops can muddy the distinction between searches and seizures. While the previous two differences do not 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.

Searches of computers typically begin when officers make an exact, complete copy of all 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." 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." Customs officers will then search the data they have mirrored, instead of the original data on the traveler's laptop. Digital searches are thus very different from analog ones. "In a 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." There is no need to return the bitstream copy to the owner; the owner has the original data in his possession all along, and the government presumably could retain the copy for extended, even infinite, 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. On the one hand, Lee Tien argues that merely copying a hard drive, without more, constitutes a seizure. When the government creates a perfect duplicate of a traveler's data, it interferes with his possessory interests in that data. Copying

136. See id. at 560–61.
137. See id. at 551.
138. Id. at 557.
139. Id. at 541.
140. See id. at 540.
141. Id. at 560.
143. Id.
information eliminates the owner’s right to exclude others and, for that reason, copying amounts to a seizure of the information. On the other hand, Professor Kerr maintains that the simple act of copying data from a hard drive is neither a search nor a seizure. He acknowledges, however, that commandeering a computer for the period of time necessary to copy the hard drive does amount to a seizure of the computer—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.”

This article does not address 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 officers may conduct many types of Fourth Amendment searches without warrant, probable cause, or even reasonable suspicion. Still, the prospect that customs officers might retain laptop data even after they have analyzed it and found nothing suspicious raises special concerns. These special concerns justify special protections that might not be necessary for traditional border searches. Part IV of this article discusses some possible additional safeguards.

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. Yet, somewhat counterintuitively, searches of laptops have the potential to be less, not more, intrusive than traditional border searches of luggage and cargo. In a standard border search, cus-
toms officers 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 proverbial needle in the haystack. In other words, the computer process separates the few 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, customs officers may not personally need to screen the great mass of information stored on a traveler's laptop. Most of the searching is done by a computer, and the computer doesn't care what the traveler looks like in his vacation photos or what he wrote in an e-mail to his wife. The officers themselves will encounter only 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. First, 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. 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. If he is paying attention, the officer 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 the traveler's friends are, he only cares whether the traveler has ties to Mohamed Atta. But exposure is an inevitable byproduct of data searches in which a hu-

149. See 9/11 COMMISSION REPORT, supra note 16, at 434. 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 nineteen of the 9/11 hijackers before the attacks. See PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE: A REPORT OF THE MARKLE FOUNDATION TASK FORCE 28 (2002), available at http://www.markle.org/downloadable_assets/nstf_full.pdf.
man being is responsible for initially scanning a data set to see if it contains anything that might merit further investigation.

Second, consider what the inspection would look like if the traveler stores his contacts electronically in Microsoft Outlook instead of a bound address book. 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 stand-alone search software like Google Desktop.\textsuperscript{150} Alternatively, the officer might import the data to a Customs computer and analyze it there.\textsuperscript{151} It is no longer necessary for the officer to review each and every one of the traveler’s contacts personally. 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 the officer only sees data that possibly suggests ties to terrorists.

Keyword searches of laptops thus potentially enable customs 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 files\textsuperscript{152}—but they can also 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. The computer restricts them to only those dis-

\begin{footnotesize}

\textsuperscript{151} See Kerr, supra note 14, at 540 (indicating that a search of computer data typically "occurs on the government’s computer, not the defendant’s").

\textsuperscript{152} But see id. at 544 ("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.").
\end{footnotesize}
tinct pieces of data flagged 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. The 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 noncontraband 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.

The same can be true for laptop searches. Just as dog sniffs help customs officers detect narcotics without rifling through the entire contents of a suitcase, keyword searches of laptops likewise enable officers 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 when customs officers want to inspect travelers' correspondence, personal diaries, or other expressive materials. Keyword searches can reduce or even eliminate the need for officers to scan hundreds of stored e-mails 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

154. See id.
155. Id. at 707.
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 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, the privacy benefits of digital searches should not be overstated. My argument is not that laptops searches are inevitably less intrusive than traditional border inspections, but rather 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, a human being will still 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 keyword searches have the potential to work well when officers are looking for text files like correspondence or contacts, they could be less effective in searches of graphic or video files that might not be keyword-searchable such as images of Osama bin Laden or video clips of child pornography. Officers may find it necessary to inspect those kinds of files manually.\footnote{156}

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." 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

\footnote{156. Professor Kerr observes that the National Drug Intelligence Center has compiled digital signatures for many known images of child pornography. Hence it may be possible to check travelers' laptops for signs of these digital signatures in a way that is similar to keyword searches. See Kerr, supra note 14, at 546.}
words, keyword searches are likely to return a number of false positives.\textsuperscript{157} 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 the owner’s suitcase.

V. 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,\textsuperscript{158} but the Constitution is not the only source of privacy protections. Policymakers in Congress or the executive branch 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 officers often perform laptop searches—by creating a bit-stream copy of a traveler’s hard drive which the government then can inspect at its discretion.\textsuperscript{159} Laptop searches thus raise the specter of officers retaining sensitive data from an entirely innocent passenger’s computer for months, maybe even years. 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.”\textsuperscript{160}

\textsuperscript{157} 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. See United States v. Diaz, 25 F.3d 392, 395 (6th Cir. 1994).

\textsuperscript{158} See United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (describing the government’s broad powers to search at the border).

\textsuperscript{159} See Kerr, supra note 14, at 557, 560–61.

\textsuperscript{160} Cf. BENVINNI 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
Collection limits seek to vindicate privacy interests in a 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 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.\textsuperscript{161} The U.S. Code offers plenty of other examples. The Foreign Intelligence Surveillance Act ("FISA") 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," such as a foreign government or terrorist organization, or an "agent of a foreign power," such as a spy or terrorist.\textsuperscript{162} 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, or sometimes necessary, to an espionage or terrorism investigation.\textsuperscript{163}

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. Rather, they seek to promote privacy by limiting what the government may do with the data it does collect, such as restricting the sharing of information or allowing it to be employed only for specified purposes. One example is the Privacy Act, which bars federal agencies from disclosing "records"—information about a person, such as financial transactions and criminal histories—unless various different exceptions apply.\textsuperscript{164} Federal Rule of Criminal Procedure 6(e)(2)(B) likewise generally prevents government lawyers and others from

\begin{footnotes}
\item[163] See 12 U.S.C. § 3414(a)(5)(A) (2006) (the 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) (2006) (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, \textit{supra} note 32, at 849–53.
\end{footnotes}
"disclos[ing] a matter occurring before the grand jury." 165 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, 166 it permits the same information to be used for other purposes. For example, the government may introduce it before a grand jury, 167 in deportation proceedings, 168 and in habeas corpus proceedings. 169

Traditional collection limits may be undesirable in some circumstances because they simultaneously can under-protect both the government's enforcement interests and the privacy interests of innocent travelers. The notion that collection limits can harm the government should be fairly intuitive. To detect crimes, the government needs information. The more information it has, the more effective its detection efforts will be—assuming, of course, that its analytical capacity is not degraded by the acquisition of additional units of data. 170 By restricting access to data that could help uncover terrorist plots, child-exploitation rings, or other crimes, collection limits can hinder the government's interest in the effective enforcement of the law. It may well be that a particular collection limit is justified as a matter of law and policy—for example, the Fourth Amendment's warrant requirement. 171 But to say that the benefits of a collection limit exceed its costs is not to say that it is costless.

166. Weeks v. United States, 232 U.S. 383, 393, 398 (1914) (holding that in a federal prosecution the Fourth Amendment barred at trial the use of evidence secured through an illegal search and seizure); see also Mapp v. Ohio, 367 U.S. 643, 655–56 (1961) (applying the exclusionary rule to the states).
170. That assumption may or may not be warranted. Like human brains, computers do not have an unlimited capacity to warehouse or process information, though the costs of storing data appear to be steadily declining. See Bellia, supra note 34, at 141, 143. The marginal cost of analyzing one additional unit of information—either by a human being or by a computer—may well be greater than zero, perhaps significantly so. Conceivably, the presence of one additional unit of information could even increase the average cost of analyzing each unit in the entire trove of data. For example, analysts or their computers may become so overloaded by the new information that it takes them longer to scrutinize the old information than it otherwise would have.
171. See Payton v. New York, 445 U.S. 573, 586 (1980) ("It is a basic principle of Fourth Amendment law that searches and seizures inside a home without a warrant are presumptively unreasonable.").
Somewhat counterintuitively, collection limits also can undermine privacy interests, at least in some cases. Standing alone, collection limits offer imperfect privacy protection. If the government is bound only by collection limits and still manages to acquire personal information, it will be able to use that data without restriction, including in ways that could undermine the subject’s privacy. The relevant collection limit might set such a low bar that customs officers can gain access to the data with very little trouble. For instance, the government may, upon a mere certification of relevance, use a pen register or trap-and-trace device to learn which numbers are dialed or received by a particular telephone.\textsuperscript{172} Or the person to whom the data pertains might consent to the government accessing it, as when a traveler lets airport security officials x-ray his carry-on as a condition of taking it onboard a plane.\textsuperscript{173} The government then can aggregate individual units of data, effectively creating “new” information that it was never authorized to collect and that the subject never consented to reveal:

> When combined together, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts. This occurs because combining information creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected.\textsuperscript{174}

Use limits—restrictions on the government’s ability to share information or employ it for purposes other than those for which it initially was collected—can help prevent these privacy harms from materializing in ways that collection limits cannot.\textsuperscript{175}

Use limits might be the best way to regulate border searches of laptop computers, for a familiar reason. Special collection limits

\textsuperscript{172} See 18 U.S.C. §§ 3122(a)-(b) (2006); see also Smith v. Maryland, 442 U.S. 735, 736, 742–44 (1979).

\textsuperscript{173} See United States v. Edwards, 498 F.2d 496, 500–01 (2d Cir. 1974).


\textsuperscript{175} This is not an argument that use limits are preferable to collections limits in all circumstances. Nor is it an argument that use limits do a better job of protecting travelers’ privacy interests in the specific context of laptop searches. One could just as easily argue that use limits should supplement, not substitute for, collection limits at the border. Rather, the purpose of the foregoing discussion is simply to highlight the different ways in which use and collection limits seek to vindicate privacy interests, and to begin to identify some of their respective strengths and weaknesses.
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." Transparency would help ensure that any abuses of laptop-search powers are corrected and thus would 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. 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 forty of the seventeen million people who entered the United States from August 1 to 13, 2008 had their laptops inspected. That is roughly equal to 960 laptop inspections.

176. Sales, supra note 32, at 816.
178. See Josh Gerstein, Feingold Bill Would Limit Searches of Travelers' Laptops, N.Y.
searches per year. The agency has also released a short document entitled “Policy Regarding Border Search of Information” (“Policy Statement”). The document sets forth rules that explain the types of electronic media that 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 the four-and-a-half-page statement lacks the detail and authority associated with other types of agency documents. Policymakers would do well to elaborate in a privacy impact assessment 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, travelers might be selected randomly. They might be chosen based on previous travel history, criminal records, the manner in which they paid for airline tickets, tips from other government agencies, or customs officers’ observations about the their demeanor. Or they may be selected based on some combination of the factors. Transparent standards would help assure people asked to undergo laptop inspections that they were selected for legitimate law-enforcement or intelligence reasons, 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.

Third, policymakers should establish protocols for resolving the false positives that will inevitably result when customs officers run keyword searches against digital data. What procedures will

180. See id. §§ (C)-(E).
182. 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.”).
the government use to tell which hits might indicate terrorism or other criminal activity and which hits are innocuous? Policymakers should make clear that, because of the risk of false positives, a search of a laptop 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. Of course, travelers should be given the opportunity to explain that the suspicious material on their laptops actually exists for innocent reasons—for example, 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 greater the inconvenience to the laptop's owner. Lengthier searches also increase the likelihood that customs officers who are hunting for contraband will, whether deliberately or by accident, start browsing through entirely innocent but sensitive computer files. It may not be practicable to establish a hard and fast rule that all laptop searches must be completed within, say, ninety minutes if performed on-site at the airport, or within forty-eight hours if the laptop is taken to an off-site computer forensics facility. At a minimum, however, customs could set targets to encourage effective yet speedy searches. Unfortunately, the Policy Statement does not do much in this regard. It merely recites the boilerplate goal that searches of laptops should be completed within "a reasonable period of time."

Policymakers also ought to adopt standards on the retention and use of data gathered during a search of a laptop. When the government hunts for evidence of crimes or national security threats, it inevitably encounters a great deal of innocent data irrelevant to its investigation. In other words, customs officers might vacuum up the entire haystack, not just the needle. Two recurring problems in surveillance law are determining (1) how to prevent the government from collecting this innocuous data and (2) how to handle the innocuous data it does sweep up. In the wiretap context, federal law manages the problem by imposing

183. POLICY STATEMENT, supra note 179, § (C)(2)(d)(2).
what are known as "minimization" requirements. For instance, the statute that governs ordinary criminal surveillance (known in the trade as "Title III") directs officers to "minimize the interception of communications not otherwise subject to interception." It also contemplates after-the-fact minimization in some cases—collection, followed by analysis, and then by destruction of data determined to be irrelevant. FISA, which governs investigations of national security threats, likewise generally requires the government to "minimize the acquisition and retention, and prohibit the dissemination," of non-public information.

Policymakers should insist on similar minimization procedures for laptop searches at the border. If an inspection fails to uncover any criminal activity, Customs would be hard-pressed to justify retaining any data from the traveler's computer. On the other hand, when the government has an obvious need to keep copies of files—for example, if the data is contraband itself or is evidence of crime—it should strictly enforce policies that limit officers' access to data and punish those who retrieve it without permission. In this vein, the 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." Hence, 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. The Policy Statement does not, how-

---

185. See id.; see also U.S. Attorney's Office, USAM: Criminal Resource Manual § 29(G) (Oct. 2008), http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00029.htm ("After-the-fact minimization is a necessity for the interception of electronic communications over a digital-display pager or a fax machine. In such cases, all communications are recorded and then examined by a monitoring agent and/or a supervising attorney to determine their relevance to the investigation.").
187. POLICY STATEMENT, supra note 179, § (C)(1); see also id. § (D)(1)(d) ("If after reviewing information, there exists no probable cause to seize the information, customs will retain no copies of the information.").
188. Id. § (D)(1)(a). 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 the Central Intelligence Agency ("CIA") to decrypt data from a traveler's laptop, the CIA may be able to keep the information even if further analysis reveals no criminal wrongdoing.
ever, 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 particularly 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 harsh penalties result for officers who access or disclose such data without authorization. Again, the Policy Statement represents a good first step. It helpfully directs customs officers to “take all reasonable measures to protect” business or commercial information “from unauthorized disclosure.” It also references the Trade Secrets Act and Privacy Act, both of which impose penalties on government employees who disclose certain types of private information. But because the Policy Statement does not offer any guidance on which protective measures count as reasonable and which do not, it likely will not offer much concrete protection. Somewhat more specifically, the Policy Statement flatly bars customs officers from searching materials “covered by attorney-client privilege” unless they first seek “advice” from Customs’s lawyers or the local U.S. Attorney’s office.

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 officers 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.” It would have the same beneficial effect for laptop searches.

189. Id. § (E)(1).
190. Id.
191. Id. § (E)(3). Customs officers need not obtain their authorization; they apparently remain free to disregard the lawyers’ advice not to search privileged materials.
VI. 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 more and more law-abiding travelers cart their computers with them when they venture abroad, and as the computers’ 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—that is, 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, they store intensely private data, and digital searches can leave a permanent copy of that 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 laptops and 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. Those standards would equip the government

---

194. Ramsey, 431 U.S. at 617.
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.