"YOUR LAPTOP, PLEASE:" THE SEARCH AND SEIZURE OF ELECTRONIC DEVICES AT THE UNITED STATES BORDER

By Sunil Bector

Since September 11, 2001 there has been an increased emphasis on border security concurrent with a period of "near exponential growth" in portable information technology.[1] Laptops and other electronic devices that contain vast amounts of sensitive data now play a central role in our daily lives and cannot easily be left behind during international travel.[2] Yet many travelers are unaware that this data may be exposed during searches of electronic devices at the border.[3] Indeed, according to Susan Gurley, the Executive Director of the Association of Corporate Travel Executives, ninety-four percent of respondents to a membership poll "were unaware that Customs or border officials can confiscate laptops for days, weeks or indefinitely."[4] If even frequent business travelers are ignorant of the extent of these border searches, lay travelers are not likely better informed.

Court cases dealing with laptop searches often have less sympathetic facts than the average criminal case. Many, for example, involve possession of child pornography, and a court inclined to give an expansive reading to the Fourth Amendment in such cases may allow an odious criminal to go unpunished. Nevertheless, the precedents established in these highly charged cases affect the privacy of all travelers. Consider a parent of a young child returning from an international business trip. The man is ran-

---

1. *See Do Privacy Rights Extend to International Travelers? Warrantless Border Searches of Electronic Devices*, 7 Privacy & Sec. L. Rep. (BNA) 279 (Feb. 25, 2008) [hereinafter *Do Privacy Rights Extend to International Travelers?*]; *see also* YULE KIM, CONG. RESEARCH SERV., CRS REPORT NO. RL31826, PROTECTING THE U.S. PERIMETER: "BORDER SEARCHES" UNDER THE FOURTH AMENDMENT 1 (2008).

2. *Do Privacy Rights Extend to International Travelers?*, *supra* note 1.

3. *Travel Executives Seek Guidance on Laptop Seizure, Content Review by Border Agents*, 5 Privacy & Sec. L. Rep. (BNA) 1502 (Oct. 30, 2006) ("The information that U.S. government officials have the right to examine, download, or even seize business travellers' [sic] laptops came as a surprise to the majority of our members.").

4. *Id.*

domly selected for an inspection when he enters the United States and the customs official turns on his laptop to discover his desktop background image depicts a naked child frolicking in a kiddie pool, which, unbeknownst to the customs officer, is the traveler's own two-year-old son. Concerned that he might possess or traffic in child pornography, the customs official confiscates his laptop, copies the contents of his hard drive, and interrogates him for several hours.[5] Satisfied that he has committed no crime, the customs official releases him. Yet, what becomes of the copied contents of the hard drive? In copying his hard drive the official may have copied trade secrets or other protected communications, in addition to personal files such as photographs and e-mails. These are some of the privacy interests at stake.

This Note will argue that invasive, suspicionless laptop searches at the border are untenable in a society where huge quantities of digital files cross the borders on laptops and digital media with increasing frequency. It is unlikely that federal courts will find stronger protection for such devices without new federal laws because, in general, searches at the border are constitutional under the Fourth Amendment.[6] In addition, most federal courts have conferred broad authority to Customs and Border Patrol (CBP) officials to search electronic devices at the border.[7] Thus, this Note contends that Congress, through legislation, should direct the Department of Homeland Security (DHS) to promulgate specific regulations regarding electronic device search and seizures at the border. This Note concludes that the Travelers' Privacy Protection Act of 2008 is a strong bill that, coupled with some additional provisions, could adequately protect the privacy of travelers while still being deferential to the government's interest in protecting its borders.

Part I of this Note lays the foundation of the border search exemption to the Fourth Amendment and considers the complexity of classifying searches as "routine" or "non-routine." Part II reviews the relevant federal appellate case law describing searches of electronic devices at the border.

---

5. This hypothetical scenario is not at all farfetched. *See* Neal Matthews, How a Photo Can Ruin Your Life, PopPhoto.com, May 4, 2007, http://www.popphoto.com/popularphotographyfeatures/4130/how-a-photo-can-ruin-your-life.html (noting that the interpretation of the intent of the content is what is often used to prosecute people).

6. *See infra* Parts I, II.

7. *Id.* Further, one's Fifth Amendment right against compelled self-incrimination may also be implicated when an individual is compelled to furnish a computer password as part of a laptop border search. *See Do Privacy Rights Extend to International Travelers*, *supra* note 1; *see also*, Declan McCullagh, *Judge orders defendant to decrypt PGP-protected laptop*, CNET NEWS, Feb. 26, 2009, http://news.cnet.com/8301-13578_3-10172866-38.html.

It also discusses *People v. Endacott*, a recent California Court of Appeal case, which gives insight into the facts and considerations necessary to analyzing cases involving electronic device searches. Part III details recent changes in the DHS's official policy regarding border searches and argues that legislation is required to implement a more transparent and just process. Part IV outlines and evaluates legislation proposed in both the 110th and early 111th Congresses and suggests guidelines for future legislation that would balance the privacy interests of travelers with the strong governmental security interest in investigating electronic storage devices.

I. THE FOURTH AMENDMENT IN THE BORDER SEARCH CONTEXT

The Fourth Amendment prohibits unreasonable search and seizure,[8] but the "border search exception" typically allows government officials to search electronic devices at the border without a warrant or probable cause.[9] Thus, Customs and Border Patrol (CBP) agents may, under current federal law, conduct "routine" searches of electronic devices without a warrant, though it is unclear what constitutes a routine search.[10] When conducting particularly invasive searches, customs officials may need to meet a higher "reasonable suspicion" standard.[11] A report released by the Congressional Research Service addresses the vagueness surrounding the degree of suspicion required to conduct a border search of an electronic storage device, noting that:

> The issue that federal courts have been confronting recently is whether the border search exception applies to electronic storage devices and, if it does, whether a laptop border search is routine or non-routine, and if found to be non-routine, what degree of suspicion or cause is needed to justify the search to satisfy the Fourth Amendment.[12]

The Fourth Amendment of the United States Constitution requires that any search warrant be supported by probable cause, with the warrant particularly describing the place to be searched and the persons or things to

---

8. U.S. CONST. amend. IV.

9. *See infra* Section I.A.

10. *Seized Laptop Contents May Be Unencrypted, Contents Shared, Under Border Patrol Policy*, 7 Privacy & Sec. L. Rep. (BNA) 1148 (Aug. 4, 2008) (reporting on United States v. Arnold, 523 F.3d 941 (2008)).

11. YULE KIM, CONG. RESEARCH SERV., CRS REPORT NO. RL34404, BORDER SEARCHES OF LAPTOPS AND OTHER ELECTRONIC STORAGE DEVICES 3 (2008).

12. *Id.* at 4.

be seized.[13] Probable cause refers to the amount of suspicion necessary for a warrant to issue, which rests somewhere between bare suspicion and the evidence needed to convict at trial.[14] An inquiry into whether one has a Fourth Amendment right not to be searched consists of two steps: (1) whether a defendant has a subjective expectation of privacy, and (2) whether society deems that the defendant's expectation of privacy is reasonable.[15] This reasonableness requirement has generally been interpreted to mean that warrantless searches are *per se* unreasonable.[16]

A. The Border Search Exception

Searches and seizures that occur at the border are exempt from these stringent Fourth Amendment warrant requirements because of the strong governmental interest in maintaining secure borders.[17] This border search

---

13. U.S. CONST. amend. IV. The Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

14. BLACK'S LAW DICTIONARY 1239 (8th ed. 2004). Black's Law Dictionary defines it as "a reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items connected with a crime." *Id.*

15. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]he rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

16. *Id.* at 357. The Court stated:

> Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes, and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.

Id. (citations omitted).

17. *See* United States v. Flores-Montano, 541 U.S. 149, 153 (2004) ("It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."); United States v. Ramsey, 431 U.S. 606, 616 (1977) ("[S]earches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border . . . ."); *see also* Jennifer M. Chacón, *Border Searches of Electronic Data*, LEXISNEXIS EXPERT COMMENTARY, June 30, 2008, at 3 ("The Supreme Court [] has upheld routine, suspicionless searches of the luggage of arriving passengers 'no matter how great the

exception, one of a number of exceptions to the Fourth Amendment, permits warrantless searches to be conducted at the border without probable cause.[18] The border search exception is based on the rationale that the governmental interest in protecting sovereign borders is far more important than an individual's privacy interest.[19] Although Congress and the federal courts assumed the exception, it was not formalized until 1977[20] when the Supreme Court, in *U.S. v. Ramsey*, approved a warrantless search conducted by a customs officer.[21] The customs agent searched a suspicious envelope at the border and found heroin.[22] The Court indicated that the official had a "reasonable cause to suspect," a standard less stringent than probable cause but sufficient for the purposes of the search.[23] "Reasonable cause to suspect" seems identical to "reasonable suspicion,"[24] which is defined as "a particularized and objective basis, supported by specific and articulable facts, for suspecting a person of criminal activity."[25]

Since *Ramsey*, the border search exception has "been expanded to not only persons, objects, and mail entering the United States by crossing past a physical border, but also to individuals and objects departing from the United States and to places deemed the 'functional equivalent' of a border, such as an international airport."[26] The functional equivalent of a border is generally defined as the first practical detention point after crossing a border, or the final port of entry.[27] The expansion of *Ramsey* is justified because, apart from the impossibility of one's physical presence at the border, it is otherwise equivalent to a border search.[28] A three-part test, established by the Eleventh Circuit, determines whether a search occurs at the border's functional equivalent by evaluating the circumstances around the search as opposed to its location.[29] Thus, a search occurs at the functional equivalent of a border when: (1) reasonable certainty exists that a border was crossed, (2) there was no opportunity for the object of the search to

---

traveler's desire to conceal the contents may be.'" (quoting United States v. Ross, 456 U.S. 798 (1982)).

18. *Ramsey*, 431 U.S. at 619.
19. *See supra* note 17.
20. KIM, *supra* note 11, at 1-2.
21. *Ramsey*, 431 U.S. at 619.
22. *Id.* at 609.
23. KIM, *supra* note 11, at 2 (citing *Ramsey*, 431 U.S. at 614).
24. *Id.*
25. BLACK'S LAW DICTIONARY 1487 (8th ed. 2004); *see also* Terry v. Ohio, 392 U.S. 1 (1978).
26. KIM, *supra* note 11, at 2.
27. KIM, *supra* note 1, at 7-8.
28. *Id.* at 8.
29. United States v. Hill, 939 F.2d 934, 937 (11th Cir. 1991).

have changed materially since the crossing, and (3) the search occurred as soon as practicable after crossing the border.[30]

In addition, the "extended border search" doctrine may also expand the border search exception beyond traditional borders and their functional equivalents.[31] In this regard, warrantless searches may be conducted if: (1) there is a reasonable certainty that a border crossing has occurred, (2) there is a reasonable certainty that the object being searched has not changed condition since crossing the border, and (3) there is a reasonable suspicion that criminal activity has occurred.[32] The third element of this test is more stringent than the functional equivalent test because the extended border search doctrine infringes more on one's reasonable expectation of privacy.[33] Nevertheless, while searches and seizures at the border and its functional equivalents are exempt from the Fourth Amendment warrant requirement, they still must be "reasonable."[34]

B. Routine v. Non-Routine Searches

Courts have categorized border searches as "routine" or "non-routine,"[35] a distinction based on the intrusiveness of the search in relation to the privacy interests of the individual being searched.[36] This can be a misleading distinction, however, because this does not seem to apply to vehicular searches.[37] Yet, generally, the more intrusive a search, the more likely it is to be considered non-routine.[38] Strip searches and body cavity searches, for example, are likely to be considered non-routine, whereas luggage searches and pat-downs are typically deemed routine.[39] Still, the Supreme Court has refused to develop a balancing test using a "routine" and "non-routine" framework, and instead notes that the terms are merely descriptive.[40]

The routine/non-routine distinction was first discussed in *United States v. Montoya de Hernandez*, where the Court found that the overnight deten-

---

30. *Id.*

31. KIM, *supra* note 1, at 8.

32. United States v. Yang, 286 F.3d 940, 946 (7th Cir. 2002) (citations omitted).

33. KIM, *supra* note 1, at 8.

34. Marsh v. United States, 344 F.2d 317, 324 (5th Cir. 1965) ("Border searches are, of course, not exempt from the constitutional test of reasonableness.").

35. KIM, *supra* note 11, at 2.

36. *See* KIM, *supra* note 1, at 7.

37. *See* United States v. Flores-Montano, 541 U.S. 149 (2004); *see also infra* text accompanying notes 45-49.

38. *See* United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006).

39. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 551 (1985).

40. United States v. Arnold, 523 F.3d 941, 945 (9th Cir. 2008).

tion of a traveler was non-routine, but justified by custom officials' "reasonable suspicion" that the traveler was smuggling drugs.[41] The Court determined that the detention was non-routine because, in part, the detention was "long, uncomfortable, and humiliating."[42] The Court held that such non-routine searches could be justified based on a "reasonable suspicion" of the officer,[43] a lower threshold than probable cause. Though *Montoya de Hernandez* dealt with the issue of detention, lower federal courts adopted the rationale of the Supreme Court, holding that routine searches may be conducted without suspicion.[44]

The Supreme Court further delineated the routine/non-routine designation and search justification standard in *United States v. Flores-Montano*.[45] The Court held that disassembly and inspection of a vehicle gas tank at the border was routine and thus did not require reasonable suspicion.[46] Although time-consuming disassembly is atypical, the Court defined a routine search as one that does not implicate increased privacy considerations.[47] Because there was no increased privacy concern surrounding the contents of an automobile gas tank, the court classified the search as routine.[48] *Flores-Montano* thus "illustrates that extensive, time-consuming and potentially destructive searches of objects and effects can be considered 'routine' and can be conducted without any necessary ground for suspicion."[49]

"Non-routine" is vaguely defined because courts typically decide what is non-routine on a case-by-case basis without resorting to a bright-line rule.[50] "Nonetheless, the holding in *Flores-Montano* indicates that, unlike

---

41. *Montoya de Hernandez*, 473 U.S. at 531.
42. *Id.*
43. *Id.*
44. *See* KIM, *supra* note 11, at 3.
45. United States v. Flores-Montano, 541 U.S. 149, 153 (2004).
46. *Id.* at 152.
47. *Id.* at 154.
48. *Id.* ("It is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobile's passenger compartment."). Moreover, the government's interest in protecting its borders was supported by strong facts:

> [S]mugglers frequently attempt to penetrate our borders with contraband secreted in their automobiles' fuel tank. Over the past 5 ½ fiscal years, there have been 18,788 vehicle drug seizures at the southern California ports of entry. Of those 18,788, gas tank drug seizures have accounted for 4,619 of the vehicle drug seizures, or approximately 25%.

Id. at 153 (citations omitted).
49. KIM, *supra* note 11, at 3.
50. *Id.*

a search of a person's body, intrusiveness may not be a dispositive factor when determining whether the search of a vehicle or personal effects is non-routine." [51] Non-routine searches require "reasonable suspicion," which in turn requires "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[52] In order to afford travelers more privacy rights, at least two commentators have recommended that laptop border searches require reasonable suspicion, [53] with one of these commentators arguing that these searches be classified as non-routine.[54]

II. THE FOURTH AMENDMENT AS APPLIED TO BORDER SEARCHES OF COMPUTERS AND OTHER ELECTRONIC DEVICES

While the Supreme Court has yet to address the Fourth Amendment protection afforded to border searches of electronic storage devices, [55] many lower courts have concluded that such searches fall under the border search exception.[56] Recent cases address whether the border search exception applies to electronic storage devices, whether these searches are routine or non-routine, and what degree of suspicion is needed to justify a non-routine search.[57] Additionally, border searches of such devices are occurring more frequently because electronic storage devices are increasingly pervasive.[58] The degree of suspicion needed to conduct a search, however, is still unclear. Despite deeming laptop searches routine, courts have also determined that the factual situations in most of these cases justified requiring reasonable suspicion to conduct a search.[59] Three major

51. *Id.* at 3-4.

52. Terry v. Ohio, 392 U.S. 1, 21 (1978).

53. *See* Christina Coletta, *Laptop Searches At The United States Borders And The Border Search Exception To The Fourth Amendment*, 48 B.C. L. REV 971 (2007); John Nelson, *Border Confidential: Why Searches of Laptop Computers at the Border Should Require Reasonable Suspicion*, 31 AM. J. TRIAL ADVOC. 137 (2007).

54. *See* Coletta, *supra* note 53.

55. Since there is no Circuit split, it seems unlikely that the Supreme Court will address the issue anytime soon. *But see* KIM, *supra* note 11, at 8 (suggesting that the Supreme Court may find laptop searches to be a suitable vehicle to outline controlling factors that determine routine v. non-routine searches).

56. *Id.* at 4; *see, e.g.*, United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006); United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006); United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005).

57. KIM, *supra* note 11, at 4.

58. *Id.*

59. *Id.*

federal appellate cases have addressed the issue of warrantless laptop searches at the border. *United States v. Ickes* stands for the proposition that laptop searches at the border do not violate the First and Fourth Amendments.[60] *United States v. Arnold* goes further by expressly stating that reasonable suspicion is not required for border searches of electronic storage devices,[61] while *United States v. Romm* extends the border search exception to deleted files that are recovered by customs officials.[62] *People v. Endacott*, a recent California Court of Appeal case, exemplifies these rules.[63]

A. Laptop Searches Do Not Violate the First and Fourth Amendments

In *United States v. Ickes*, the Fourth Circuit held that the warrantless search of Ickes's van, including his computer and disks, did not violate the First or Fourth Amendments.[64] Upon entering the United States from Canada, John Ickes's van was subject to a "cursory" routine search after informing a U.S. Customs Inspector that he was returning from vacation, even though his van "appeared to contain 'everything he owned.'"[65] The inspector instituted a more comprehensive search after viewing a suspicious video of a tennis match focusing excessively on a young ball boy,[66] and found marijuana paraphernalia, a previous arrest warrant, a computer, seventy-five computer disks, and a photo album depicting child pornography.[67] After being charged with transporting child pornography, Ickes filed a motion to suppress the recovered evidence, arguing that the warrantless search of his van violated both the Fourth and First Amendments, invoking the latter by arguing that the search involved expressive material.[68] The Fourth Circuit upheld the warrantless search of Ickes's vehicle under the border search exception[69] and dismissed the First Amendment claim for its untenable national security implications and administrative burdens.[70] Ickes complained that the sweeping ruling meant that "any per-

60. *Ickes*, 393 F.3d at 502.
61. 523 F.3d 941, 946 (9th Cir. 2008).
62. *Romm*, 455 F.3d 990, 1006 (9th Cir. 2006).
63. 79 Cal. Rptr. 3d 907, 908-910 (Ct. App. 2008).
64. *Ickes*, 393 F.3d at 502.
65. *Id.*
66. *Id.*
67. *Id.* at 503.
68. *Id.* at 503-05.
69. *Id.* at 505.
70. *Id.* at 506 ("[N]ational security interests may require uncovering terrorist communications, which are inherently 'expressive.' Following Ickes's logic would create a sanctuary at the border for all expressive material—even for terrorist plans.").

son carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer hard drive."[71] The court, noting that "Customs agents have neither the time nor the resources to search the contents of every computer,"[72] responded that "[a]s a practical matter, computer searches are most likely to occur where—as here—the traveler's conduct or the presence of other items in his possession suggest the need to search further."[73] Thus, the court noted that computer searches would likely only occur upon reasonable suspicion due to practical considerations.[74] However, the court did not *require* reasonable suspicion to conduct laptop searches.

B. Laptop Searches Do Not Require Reasonable Suspicion

In *United States v. Arnold*, the Ninth Circuit went further than the *Ickes* court by expressly holding that electronic storage device searches at the border do not require reasonable suspicion.[75] Leading up to this important decision, the United States District Court for the Central District of California held that officers must have reasonable suspicion to conduct a laptop search.[76] Michael Arnold returned from the Philippines to Los Angeles International Airport, where CBP officials selected him for questioning and subjected him to a luggage search.[77] During the luggage search, the CBP officials asked Arnold to turn on his computer, which he did. After a search of his desktop files revealed an image of two nude women,[78] ICE agents were summoned to further question Arnold. They eventually released Arnold but seized his computer and other electronic storage devices on suspicion of possession of child pornography.[79] Arnold argued

---

71. *Id.* at 506-07.

72. *Id.* at 507. While this is not the court's main point, it is likely that scanning software will become faster and more efficient as time goes on, thereby making it more likely that every computer can be searched.

73. *Id.*

74. *Id.* The court continues:

> However, to state the probability that reasonable suspicions will give rise to more intrusive searches is a far cry from enthroning this notion as a matter of constitutional law. The essence of border search doctrine is a reliance upon the trained observations and judgments of customs officials, rather than upon constitutional requirements applied to the inapposite context of this sort of search.

Id.

75. United States v. Arnold, 523 F.3d 941, 946 (9th Cir. 2008).

76. United States v. Arnold, 454 F. Supp. 2d 999, 1001 (C.D. Cal. 2006).

77. *Arnold*, 523 F.3d at 943.

78. "The government [did] not present[] evidence that the photo depicted minors." *Arnold*, 454 F. Supp. 2d at 1001 n.1.

79. *Arnold*, 523 F.3d at 943.

that this evidence should be suppressed because the search was conducted without reasonable suspicion, to which the government replied that (1) the border search exception applied, and (2) reasonable suspicion was present.[80] The court did not believe reasonable suspicion existed due to the inadequacy of the government's testimony at trial,[81] and concluded that a laptop search required reasonable suspicion.[82] The district court specifically held that the search of Arnold's laptop was non-routine,[83] a move lauded by at least two commentators advocating for more a more stringent standard for electronic data searches.[84]

However, on appeal, the Ninth Circuit overruled the district court, determining that the intrusiveness of a laptop search is not significant enough to invoke the reasonableness requirement of the Fourth Amendment.[85] Arnold argued that reasonable suspicion was necessary because laptops can store huge quantities of information and, thus, they are more comparable to one's home or the human mind than a closed container.[86] The court, noting the long history enabling border searches of closed containers without particularized suspicion,[87] likened laptops to other pieces of property and held that no reasonable suspicion is needed to search laptops or other electronic storage devices.[88] The court rejected Arnold's analogy equating a laptop search to that of a home and concluded that a search cannot be "particularly offensive" simply due to the object's sto-

80. *Id.*

81. *Arnold*, 454 F. Supp. 2d at 1004. "[T]he government . . . [did] not provide[] the Court with any record of the search that was completed at or near the time of the incident." *Id.* Moreover, a "memorandum, written nearly a year after the search, . . . [was the CBP official's] only memorialized account of the incident." *Id.* The court noted that "[a] search is reasonable in scope only if it is no more intrusive than necessary to obtain the truth respecting the suspicious circumstances." *Id.* at 1003 (citation omitted).

82. *Arnold*, 523 F.3d at 943.

83. *Arnold*, 454 F. Supp. 2d at 1003.

84. *See* Coletta, *supra* note 53; Nelson, *supra* note 53.

85. *Arnold*, 523 F.3d at 946.

86. *Id.* at 944.

87. *Id.* at 945.

88. *Id.* at 946. This is not to say that all property can be searched at the border without reasonable suspicion. The court stated that the Supreme Court has carved out two exceptions to this rule. One, if the search involves "exceptional damage to property" or, two, if the search is carried out in a "particularly offensive manner." *Id.* at 946. The court determined that neither of these exceptions applied. *Id.* at 947.

rage capacity.[89] Both a petition for rehearing and a petition for rehearing en banc were denied.[90]

C. Deleted Files May be Recovered by Customs Officials

In *United States v. Romm*, the Ninth Circuit held that recovering deleted files on a laptop computer with neither a warrant nor probable cause fell under the border search exception to the Fourth Amendment.[91] Stuart Romm's laptop was first searched by Canadian officials while trying to enter Canada after agents discovered that he had a criminal history.[92] The search revealed child pornography websites in the laptop's web browser history and Romm was denied entry to Canada and deported to Seattle.[93] In Seattle, Romm was detained by Immigration and Customs Enforcement (ICE) officials, and he agreed to a deeper inspection of his laptop.[94] ICE officials recovered deleted child pornography on Romm's laptop, the results of which Romm unsuccessfully tried to suppress at trial.[95]

The Ninth Circuit reasoned that: (1) international airport terminals are the "functional equivalent[s]" of borders, thereby allowing customs officials to search deplaning passengers, and (2) the search of Romm's laptop was supported by reasonable suspicion.[96] Romm argued that the search should be considered non-routine, but the court declined to address this contention on procedural grounds as Romm raised this argument for the first time in his reply brief.[97]

D. *People v. Endacott*

In *People v. Endacott*, the Second Appellate District Court of Appeal of California used *Flores-Montano, Ickes,* and *Arnold* to conclude that a search of the defendant's electronic devices was valid under the border search exception.[98] The defendant, Endacott, arrived from Thailand at Los

89. *Id.* at 947.

90. *See New House Bill Would Ban Border Searches of Laptops Based on U.S. Sovereign Authority*, 7 Privacy & Sec. L. Rep. (BNA) 1115 (July 28, 2008) [hereinafter *New House Bill*].

91. 455 F.3d 990, 1006 (9th Cir. 2006).

92. *Id.* at 994.

93. *Id.*

94. *Id.* Canada's Border Services Agency tipped off U.S. Customs, informing them that Romm had (1) been denied entry into Canada, and (2) was possibly in possession of illegal images.

95. *Id.* at 996.

96. *Id.* at 996-97.

97. *Id.* at 997 ("[A]rguments not raised by a party in its opening brief are deemed waived") (quotations omitted).

98. People v. Endacott, 79 Cal. Rptr. 3d 907, 908-910 (Ct. App. 2008).

Angeles International Airport on September 29, 2006.[99] Endacott was interrogated during a routine customs inspection, during which he revealed that he had been in Thailand for four months resting, visiting a friend, and seeking employment.[100] The customs agent thought it unusual that Endacott carried plastic cases and arrived in a leather jacket and gloves when returning from such a warm climate.[101] The customs agent sent Endacott for secondary inspection where another agent received a "binding declaration" from Endacott averring that he was the owner of all items in his possession.[102] Because Thailand is a country "considered to be a high risk for child pornography," Endacott's two laptop computers were searched for pictures and videos.[103] The search queries produced images of preadolescent nude females whom Endacott identified as fourteen-year-old models.[104] Endacott claimed that the images were legal because they were obtained from a "legal website."[105] Agents confiscated Endacott's computers and other digital media and Endacott provided consent for additional searches.[106] Two days later a special agent discovered thousands of "images of pubescent and prepubescent girls in various states of undress" on one of the laptops.[107] A search of two external hard drives turned up over ten thousand additional images.[108] The court held that the searching of Endacott's belongings was valid under the border search exception.[109] While the trial court held that the search was "without probable cause or even a reasonable suspicion," the search was upheld as a routine border search.[110]

Endacott argued that (1) his laptop search violated the Fourth Amendment because there was no reasonable suspicion, and (2) the expressive materials hosted on his laptop entitled it to greater protection than other articles searchable at borders.[111] The court dismissed the first claim by citing the Supreme Court in *United States v. Flores-Montano*[112] and held that

---

99. *Id.* at 908.
100. *Id.*
101. *Id.*
102. *Id.* Endacott later consented to a search of his computers and digital media.
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *See id.*
111. *Id.* at 908-09.
112. 541 U.S. 149, 152 (2004) ("[S]earches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons

border searches are reasonable simply because they occur at the border.[113] The court countered Endacott's second claim by citing the Fourth Circuit in *United States v. Ickes*,[114] where the court rejected a similar expressive materials argument by noting that expressive materials could contain terrorist communications and that creating an exception for such materials would "defeat the purpose of the border search doctrine, which is to allow the sovereign to protect itself."[115] The court then cited two cases holding that computers should be treated like other containers for the purposes of search and seizure laws.[116] The court ended with an analogy:

> Indeed, the human race has not yet, at least, become so robotic that opening a computer is similar to a strip search or body cavity search. Of course viewing confidential computer files implicates dignity and privacy interests. But no more so than opening a locked brief case, which may contain writings describing the owner's intimate thoughts or photographs depicting child pornography. A computer is entitled to no more protection than any other container. The suspicionless border search of Endacott's computer was valid.[117]

Thus, the *Endacott* case is simply one of the latest in a line of decisions affirming warrantless electronic device searches.

III. THE DEPARTMENT OF HOMELAND SECURITY AND ITS BORDER SEARCH POLICIES

Because numerous courts have vindicated CBP's broad authority to search individuals and their electronics at the border,[118] it is relevant to examine how CBP obtained its authority. Much of it came from the Homeland Security Act,[119] passed in 2002, which established the Department of Homeland Security to, among other things, "prevent terrorist attacks within the United States, . . . carry out all functions of entities transferred to the Department, . . . [and] monitor connections between illegal drug

---

and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977))).

113. *See Endacott*, 79 Cal. Rptr. 3d at 909.

114. 393 F.3d 501 (4th Cir. 2005).

115. *Endacott*, 79 Cal. Rptr. 3d at 909.

116. *Id.* at 909.

117. *Id.*

118. *See supra* Part II.

119. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of U.S.C.).

trafficking and terrorism."[120] The Act established the Directorate of Border and Transportation Security, who is responsible for:

> [p]reventing the entry of terrorists and the instruments of terrorism into the United States. . . . [s]ecuring the borders . . . [and] [e]stablishing and administering rules . . . governing the granting of visas or other forms of permission . . . to enter the United States to individuals who are not a citizen or an alien lawfully admitted for permanent residence in the United States,[121]

as well as "ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce."[122] Pursuant to the Homeland Security Act, the United States Customs Service, Transportation Security Administration, and several other agencies were transferred to the DHS.[123] Because the DHS now effectively controls the borders, it is important to consider its border search policies.

On July 16, 2008, the DHS, in an effort to be more transparent,[124] publicized its "long-standing" policy regarding border searches of documents, computers, and other electronic devices, stating that:

> [i]n the course of a border search, and absent individualized suspicion, officers can review and analyze the information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States, subject to the requirements and limitations provided herein. Nothing in this policy limits the authority of an officer to make written notes or reports or to document impressions relating to a border encounter.[125]

The five-page document, in essence, confers authority to border officials to peruse electronic devices without any suspicion of criminal activity whatsoever. DHS officials are entitled to "detain" electronic devices for a "reasonable period of time," on-site or off-site.[126] The policy does not define a "reasonable period of time."[127] Further, absent individualized

---

120. 6 U.S.C. § 111 (2006).
121. 6 U.S.C. § 202 (2006).
122. *Id.*
123. 6 U.S.C. § 203 (2006).
124. Ellen Nakashima, *Expanded Powers to Search Travelers at Border Detailed*, WASH. POST, Sept. 23, 2008, at A2.
125. U.S. Customs & Border Prot., Policy Regarding Border Search of Information (July 16, 2008), U.S. Customs and Border Protection, http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf.
126. *Id.*
127. *Id.*

suspicion, officials may share copied information with other Federal agencies or entities in order to "seek translation and/or decryption assistance."[128] Officers can, for example, seek assistance from the NSA to break any encrypted files on one's electronic device even if there is no suspicion of criminal activity. With supervisory approval, and with reasonable suspicion, customs officials may also seek assistance from other agencies and entities if subject matter experts are required to investigate the information.[129] These agencies are entitled to retain the information for the period of time needed to offer assistance.[130] If probable cause develops during this initial search, officials are authorized to seize documents and devices.[131]

Further, the policy outlines how the DHS intends to protect sensitive information. If officials encounter business or commercial information, "all reasonable measures to protect that information from unauthorized disclosure" shall be taken.[132] No further detail is provided on what constitutes "reasonable measures," however.[133] If the attorney-client privilege is invoked, "special handling procedures" may apply, though "legal materials are not necessarily exempt from a border search."[134] Finally, if no probable cause exists after conducting a search, copies of all information retained must be destroyed unless the matter relates to immigration, though the time frame for destruction is not defined.[135]

The Asian Law Caucus (ALC) and Electronic Frontier Foundation (EFF) have criticized the DHS's policy for the lax privacy protection required for searches and seizures, also noting that these practices deviate significantly from previous government practices.[136] According to the ALC, search polices were first enacted in 1986 by the Reagan administration to counter lawsuits initiated by U.S. citizens interrogated and searched after returning from Nicaragua.[137] In 1986, border search policy enabled officials to detain materials based on reasonable suspicion of illegal activi-

---

128. *Id.*
129. *Id.*
130. *Id.*
131. If the information concerns immigration, no probable cause is needed. *Id.*
132. *Id.*
133. *Id.*
134. *Id.*
135. *Id.*
136. *See* Bob Egelko, *Feds Give Customs Agents Free Hand to Seize Travelers' Documents*, S.F. CHRON., Sept. 24, 2008, at A6; *see also* Nakashima, *supra* note 124 (noting that from 1986 until 2007, probable cause was necessary to copy materials crossing the border).
137. Egelko, *supra* note 136.

ty, or seize and copy materials if there was probable cause to do so.[138] The Clinton administration updated border search policies in 2000 but made no significant changes.[139] The next significant change came in July 2007 when the Bush administration eliminated the reasonable suspicion requirement, removing a significant barrier to border searches.[140] Previously, customs agents could "glance" at documents in order to ascertain whether illegal goods were being trafficked without any suspicion, but reasonable suspicion was required to confiscate and read any documents.[141] The ALC protested:

> For more than 20 years, the government implicitly recognized that reading and copying the letters, diaries, and personal papers of travelers without reason would chill Americans' right to free speech and free expression . . . . But now customs officials can probe into the thoughts and lives of ordinary travelers without any suspicion at all.[142]

Jennifer Chacón, a law professor at the University of California, Davis, notes that CBP's broad authority carries three potential risks.[143] First, international travelers have no assurance that information on their electronic storage devices will not be reviewed or stored by the government.[144] Second, business travelers using company computers may be held accountable for the contents of those computers, regardless of whether they created it.[145] Third, border searches without reasonable suspicion may lead to searches that are arbitrary, unnecessary, or involve racial profiling.[146] Indeed, the ALC has noted that they have received increasing reports from travelers complaining of being questioned about their religious and political persuasions.[147]

David Cole, a law professor at Georgetown University, succinctly addresses the privacy issues surrounding laptop searches:

> It's one thing to say it's reasonable for government agents to open your luggage . . . . It's another thing to say it's reasonable

138. Nakashima, *supra* note 124.
139. Egelko, *supra* note 136.
140. Nakashima, *supra* note 124.
141. Egelko, *supra* note 136.
142. *Id.*
143. Chacón, *supra* note 17, at 9.
144. *Id.* at 9-10 (footnote omitted).
145. *Id.* at 10 (footnote omitted).
146. *Id.*
147. Nakashima, *supra* note 124.

> for them to read your mind and everything you have thought over the last year. What a laptop records is as personal as a diary but much more extensive. It records every Web site you have searched. Every e-mail you have sent. It's as if you're crossing the border with your home in your suitcase.[148]

Legislative reform should attempt to address all these issues.

IV. LEGISLATIVE ATTEMPTS AT REFORM

Concerned by the high level of intrusion constitutionally allowed during border searches, compounded with little privacy protection afforded to travelers under DHS policy, privacy advocates have urged the DHS to establish rules requiring reasonable suspicion of illegal activity prior to searching electronic devices.[149] In response to pressure from advocacy groups and their own concerns, elected representatives have responded to critics of the DHS's border search policies by introducing various legislative proposals in the 110th and 111th Congresses.[150]

A. Proposed Legislation[151]

Elected officials proposed four bills in 2008. Representative Zoe Lofgren, a Democrat from California, introduced the "Electronic Device Privacy Act of 2008" (110 H.R. 6588) on July 23, 2008 (Lofgren bill).[152] The following week, on July 31, 2008, eleven bipartisan co-sponsors, including New York Democrat Representative Eliot Engel, introduced the "Securing Our Borders and Our Data Act of 2008" (H.R. 6702) in the House (Engel bill).[153] Rep. Engel reintroduced this bill unchanged in the 111th Congress on January 7, 2009.[154] On September 11, 2008, nine Democrats, including California Representative Loretta Sanchez, introduced the "Border Security Search Accountability Act of 2008" in the House (H.R. 6869) (Sanchez bill).[155] Finally, on September 26, 2008, the United States House

148. Ellen Nakashima, *Clarity Sought on Electronics Searches*, WASH. POST, Feb. 7, 2008, at A1.

149. *New House Bill*, *supra* note 90.

150. Because none of these proposals passed in 2008, elected officials will have to reintroduce legislation in the 111th Congress in 2009.

151. Section IV.A includes legislation introduced prior to March 1, 2009.

152. Electronic Device Privacy Act of 2008, H.R. 6588, 110th Cong. (2008). *See also New House Bill*, *supra* note 90.

153. *Senate, House Democrats Offer Bills To Limit Border Searches of Laptops*, 7 Privacy & Sec. L. Rep. (BNA) 1437 (Oct. 6, 2008) [hereinafter *Senate, House Democrats*].

154. Securing Our Borders and our Data Act of 2009, H.R. 239, 111th Cong. (2009).

155. *Senate, House Democrats*, *supra* note 153.

and Senate introduced the "Travelers' Privacy Protection Act of 2008," which appears to be the strongest and most comprehensive of the group (Feingold bill).[156]

The Lofgren bill, which had no co-sponsors as of September 30, 2008,[157] would prevent CBP agents from conducting warrantless border searches of laptop computers and other electronic devices.[158] Officials would be unable to rely solely on sovereign authority, often cited by courts, to conduct laptop searches. Instead, border officials would have to be granted the authority specifically by statute.[159] Support of this bill, as evinced by a lack of co-sponsors, seems unlikely since the sixteen-line text of the bill completely eradicates the ability of officials to search electronic devices by drawing on the authority of the United States based on its power as sovereign. Although this bill does afford ample privacy protection to travelers crossing the border in that they will likely not be searched at all, it does not appear to confer any authority on United States border officials to investigate non-routine scenarios based on reasonable suspicion. However, the bill does add the caveat that searches based on other lawful authority will not be prohibited.[160] Still, the bill seems politically unfeasible and thus is not likely to move.

The Engel bill, along with the Sanchez bill, both task the Secretary of the DHS with promulgating regulations on laptop border searches.[161] Under the Engel bill, electronic data searches must be supported by reasonable suspicion, seizures must be based on some constitutional authority other than the power of the sovereign, officers must be appropriately trained to prevent damage to and deletion of data from devices, and travelers may be required to turn on devices to ensure they are operational.[162] Searches must be conducted in the presence of a supervisor, and travelers may request that the search be conducted privately.[163] The bill also outlines issues that the DHS must consider, such as policies for protecting the

156. Travelers' Privacy Protection Act of 2008, S. 3612, 110th Cong. § 4 (2008), Travelers' Privacy Protection Act of 2008, H.R. 7118, 110th Cong. § 4 (2008). The Act was introduced in the Senate by Wisconsin Senator Russell Feingold.

157. *Id.*

158. H.R. 6588 § 2; *see also New House Bill*, *supra* note 90.

159. *New House Bill*, *supra* note 90.

160. H.R. 6588 § 2.

161. Border Security Search Accountability Act of 2008, H.R. 6869, 110th Cong. § 2 (2008); Securing Our Borders and Our Data Act of 2008, H.R. 6702, 110th Cong. § 2 (2008); *see also Senate, House Democrats*, *supra* note 153.

162. Securing Our Borders and Our Data Act of 2008, H.R. 6702, 110th Cong. § 2 (2008).

163. *Id.*

integrity of data, for the duration, location, and other circumstances surrounding seized data, for the sharing of downloaded information with other agencies, and for the rights of an individual to ensure return of confiscated data.[164] The DHS is also required to give a receipt to those whose device has been seized providing contact information to follow-up, and the DHS must place all these rules on its public website.[165] Finally, the DHS must conduct an annual study of searches and seizures, including the number of searches and seizures, the race, gender, and national origin of the travelers subject to those searches, the type of searches conducted, and the results of the searches.[166] These findings must then be presented to Congress.[167]

The Sanchez bill builds on the Engel bill in its specificity of the rules to be considered. Any information determined to be commercial, ranging from trade secrets to attorney-client privilege, "shall be handled consistent with the laws, rules, and regulations governing such information and shall not be shared with a Federal, State, local, tribal, or foreign agency unless it is determined that such agency has the mechanisms in place to comply with such laws, rules, and regulations."[168] While the Engel bill *requires* searches to be conducted in front of a supervisor, the Sanchez bill merely states that supervisors must be present "to the greatest extent practicable."[169] However, the Sanchez bill allows, "where appropriate," travelers to be present when their electronic device is being searched.[170] While both bills require officials to be trained, the Sanchez bill also provides for an auditing mechanism to ensure that officials are conducting searches in accordance with the rules. Further, the Sanchez bill requires the DHS to outline limitations on warrantless searches, such as the length of time electronic devices could be detained absent probable cause, and requires the destruction of information after a specified time period.[171] If information is copied, shared, retained, or entered into a database, the owner of said information must be notified in writing, absent national security implications. Moreover, DHS officials must also prepare both a privacy impact assessment as well as a civil liberties assessment of the proposed rules.

164. *Id.*
165. *Id.*
166. *Id.* § 3.
167. *Id.*
168. H.R. 6869 § 2.
169. *Id.*
170. *Id.*
171. *Id.*; *see also Senate, House Democrats*, *supra* note 153.

The other provisions in the Sanchez bill are similar to the Engel bill. Overall, the Sanchez bill is stronger than both the Engel and Lofgren bills.

The Feingold bill, which aims to provide standards for border search and seizures of electronic devices,[172] incorporates many elements of the previous bills while also building on them, thereby making it the most comprehensive and specific bill in the group. The bill covers "law-abiding"[173] citizens and legal residents of the United States and requires that CBP officials have reasonable suspicion before searching electronic devices and probable cause before seizing equipment.[174] The Act disputes that the privacy of information stored in laptops is akin to that of "closed containers" on several grounds.[175] The Act emphasizes that laptops "can contain the equivalent of a full library of information about a person,"[176] and that "searches of electronic equipment [are] more invasive than searches of physical locations or objects."[177] Further, the legislation discourages profiling, stating that "[t]argeting citizens and legal residents of the United States for electronic border searches based on race, ethnicity, religion, or national origin is wholly ineffective as a matter of law enforcement and repugnant to the values and constitutional principles of the United States."[178] This finding is enforced by a prohibition on profiling in the bill, though it is diluted somewhat by creating an exception for profiling when a customs official has reasonable suspicion based on other factors.[179] Procedurally, all searches would require prior authorization by a supervisor and the scope of the search would be limited to the reasonable suspicion recorded.[180] The bill also requires that copies of information retained by customs officials or other agencies conscripted to help evaluate the information be destroyed within three days if no seizure occurs.[181] Perhaps most unique to the Feingold bill is its enforcement procedures. The bill not only provides for compensation measures for damages due to a search, but also enables civil actions for violations of the bill, giving the

172. Travelers' Privacy Protection Act of 2008, S. 3612, 110th Cong. § 4 (2008); Travelers' Privacy Protection Act of 2008, H.R. 7118, 110th Cong. § 4 (2008).

173. It is not clear what is meant by "law-abiding."

174. S. 3612 § 4(a); H.R. 7118 § 4(a).

175. S. 3612 § 2(4); H.R. 7118 § 2(4).

176. S. 3612 § 2(4)(A); H.R. 7118 § 2(4)(A).

177. S. 3612 § 2(4)(C); H.R. 7118 § 2(4)(C).

178. S. 3612 § 2(8); H.R. 7118 § 2(8).

179. S. 3612 § 7(b); H.R. 7118 § 7(b).

180. S. 3612 §§ 5(a)(1), 5(b)(3)(c)(1); H.R. 7118 §§ 5(a)(1), 5(b)(3)(c)(1).

181. S. 3612 § 5(b)(3)(e)(2); H.R. 7118 § 5(b)(3)(e)(2).

Feingold bill actual teeth compared to the other bills.[182] Plaintiffs' attorney fees are also available at a judge's discretion.[183]

B. Better Legislation

Ideal legislation would combine elements of the Sanchez bill with the Feingold bill, along with a few other substantive changes. The Feingold bill, alone, is a good compromise between the strong governmental interest in protecting the borders and the privacy interests retained by individuals that are recognized and protected by the Fourth Amendment. The bill allows government officials to conduct searches without the onerous burden imposed by the warrant requirement, but imposes additional restraints on government officials to keep them from abusing this power.[184] For instance, under the bill the government may only retain electronic devices for a limited amount of time, absent probable cause.[185] The Feingold bill takes profiling seriously by explicitly prohibiting it, albeit with a large exception, but also enabling plaintiffs to protest alleged profiling with favorable evidentiary rules.[186] The Feingold bill also provides a timetable for returning seized devices to individuals and for destroying copied materials.[187] Further, the bill covers electronic devices generally, rather than covering only laptops—a provision crucial to address technological innovation as portable electronic devices increase in capacity and prevalence.[188]

While the Feingold bill adds a number of effective limitations on government intrusion, there are further structural changes that could strengthen the bill by providing additional privacy protections without compromising the government's interests. Ideal legislation would detail not only when materials are eliminated, but how they are eliminated, as the Sanchez bill provides. The Feingold bill requires that the DHS maintain detailed records of each border search, but it makes no provision for making

182. S. 3612 § 12; H.R. 7118 § 12. Moreover, in an effort to stymie profiling, the bill provides that "proof that searches of the electronic equipment of United States residents at the border have a disparate impact on racial, ethnic, religious, or national minorities shall constitute prima facie evidence of the violation." S. 3612 § 12(a)(4); H.R. 7118 § 12(a)(4).

183. "In any civil action filed under paragraph (1), the district court may allow a prevailing plaintiff reasonable attorney's fees and costs, including expert fees." S. 3612 § 12(a)(5); H.R. 7118 § 12(a)(5).

184. S. 3612 § 5; H.R. 7118 § 5.

185. S. 3612 § 5(e); H.R. 7118 § 5(e).

186. S. 3612 § 12(a)(4); H.R. 7118 § 12(a)(4).

187. S. 3612 § 6; H.R. 7118 § 6.

188. S. 3612 § 3(4); H.R. 7118 § 3(4).

information available to Congress or the public.[189] The release of such records could act as an additional safeguard to check the power of CBP officials. Further, provisions in the Sanchez bill could boost the Feingold bill by explicitly establishing requirements for commercial information, such as trade secrets, attorney-client privilege, and work product. By far the biggest loophole in any proposed legislation thus far, however, is that they neglect to cover non-U.S. citizens or residents. For example, under the Feingold bill, an Indian employee of a multinational corporation could be subject to a more intrusive search than an American employee, even though a search of either of their laptops might reveal trade secrets.

V. CONCLUSION

The governmental interest in searching electronic devices is strong. Laptop searches seek both physical contraband, such as drugs and weapons, as well as information contraband, such as international espionage and child pornography. Using the latter as an example, single, white, male, non-business travelers to Southeast Asia are sometimes suspected to be sex tourists. Because trying to prove child molestation, an extraterritorial law, is nearly impossible since the government has to prove that the defendant engaged in or had the intent to engage in molestation, and because child molesters tend to horde pornography, it is much easier to search the laptops of suspicious individuals at the border. Instead of pursuing child pornographers internationally, why not just search them at the border? Child pornography possession is a strict liability crime; this is the easiest way.

Yet, there are immense privacy issues at stake as electronic devices hold lifelong libraries of information. Moreover, this is not solely a border search issue but one of profiling. Given the DHS's recent clarification of their broad authority to conduct electronic device border searches, and given the court's willingness to confer broad authority to CBP officials, it is up to Congress to set the standard by which the country can ensure its security while simultaneously protecting the privacy rights of travelers.[190]

---

189. S. 3612 § 5(a)(2); H.R. 7118 § 5(a)(2).

190. That said, the DHS's own Data Privacy and Integrity Advisory Committee, in a letter dated February 5, 2009, recommended to DHS Secretary Janet Napolitano that the DHS integrate privacy protections into the border search process. *See* Letter from J. Howard Beales, Chair, DHS Data Privacy & Integrity Advisory Comm., to Janet Napolitano, Sec'y, DHS (Feb. 5, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_letter_sec_and_acpokropf_2009-02-05.pdf. The Committee states:

Strengthening the Travelers' Privacy Protection Act by incorporating provisions from the Border Security Search Accountability Act, as well as providing privacy protection for non-U.S. citizens and residents, will ensure that the government has adequate reach to protect the homeland country while also securing sufficient privacy rights for travelers. In the interim, it may very well be best for international travelers to either leave their laptops and electronic storage devices at home, or wipe them of confidential information before traveling.[191]

> While certain DHS components may have legal authority to conduct border searches, there is a significant difference between looking at paper documents and searching through the volume of digital information that can be carried by travelers. The Privacy Office should have a role in reviewing current policies and practices for searches and seizures of digital information and developing guidelines to integrate privacy protections into these processes.

Id. Still, legislation is the better solution since it is enforceable and has reporting provisions. *See supra* Part IV.

191. Indeed, some companies are advising their employees not to carry confidential information with them on international trips. *See* Nakashima, *supra* note 148.