UCLA LAW REVIEW

# "Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices

Sid Nadkarni

## ABSTRACT

The Fourth Amendment's border search doctrine has historically given the U.S. government the right to search, without individualized suspicion, the belongings of any individual crossing the U.S.border. Courts have traditionally justified this power by citing the government's paramount interest in preventing the smuggling of dutiable goods and contraband such as illegal drugs. In the twenty-first century, the government has controversially used this power to search and detain travelers' portable electronic devices, such as laptop computers, without suspicion to inspect for the transport of prohibited materials like child pornography, terrorist communications, and pirated software.

In March 2013, the Ninth Circuit in *United States v. Cotterman* became the first federal circuit court to rule that a particular border search of an electronic device had to be preceded by a finding of reasonable suspicion that the individual had committed a crime. Nonetheless, divergent rulings from the Fourth Circuit and a Massachusetts federal district court leave the future of digital border searches shrouded in legal uncertainty. Furthermore, the Department of Homeland Security's recent reaffirmation of its view that no suspicion at all is required for such searches puts the government on a legal collision course with the Ninth Circuit and any other jurisdiction that adopts a similar position.

This Comment argues that digital border searches merit greater scrutiny than conventional border searches because they are more likely to harm individuals' Fourth Amendment interests. The executive and legislative branches have been unwilling and unable, respectively, to cabin the government's power to search people's electronic devices without suspicion. Consequently, this Comment proposes that courts add guidance, consistency, and greater Fourth Amendment protection to the laws governing suspicionless digital searches at the border by adopting a special needs–style balancing test that weighs the government's interests against the individual's and provides that the most intrusive searches are impermissible without reasonable suspicion.

## AUTHOR

Sid Nadkarni, J.D. Candidate, UCLA Law Class of 2014, is an Associate Editor of the *UCLA Law Review*, Volume 61.

I would like to thank Professors Devon Carbado and Adam Winkler for the advice and feedback they provided in choosing the topic of this Comment and in helping refine my ideas. I would also like to thank Kari Hicks for the many hours she spent editing my work and for her countless excellent suggestions. Additionally, I thank Makoa Kawabata for humorously inspiring the title of this Comment. Finally, I am grateful to the Honorable Kim McLane Wardlaw and her clerks for giving me the opportunity to extern at the Ninth Circuit Court of Appeals in summer 2012, where I was able to observe the hearings that sparked my interest in this topic.

## TABLE OF CONTENTS

Introduction....148
I. The History and Justification of Suspicionless Searches....155
A. Ordinary Fourth Amendment Jurisprudence....155
B. Permissible Suspicionless Searches....156
II. Border Searches....159
A. Border Searches Presently Requiring Reasonable Suspicion....161
B. Courts' Varying Treatment of Border Searches of Personal Electronic Devices....162
C. Consequences of the Interjurisdictional Split....165
D. Framing Digital Border Searches as Special Needs Searches....167
III. Analyzing the Impact of Digital Border Searches Under the Status Quo....168
A. Are Searches of Portable Electronic Devices Meaningfully Different From Searches of Nondigital Containers?....168
1. Should Storage Capacity Impact Permissibility?....169
2. Portable Devices' Tendency to Contain Personal Information....171
B. Unique Risks to Privacy Posed by Searches of Portable Electronic Devices....171
C. How Is Current Government Policy on Laptop Border Searches Impacting These Privacy Concerns?....177
D. Past Legislative Proposals to Regulate Border Searches of Electronic Devices....179
IV. When Should Reasonable Suspicion be Required for a Digital Border Search?....180
A. Special Needs–Style Balancing Test....181
1. The Government's Interest—Does the Search Serve a Special Need?....183
a. Digital Versus Physical Contraband....184
2. Calculating the Fourth Amendment Interests Infringed by Electronic Border Searches....186
B. Arguments for Categorical Permission of Suspicionless Digital Border Searches....191
Conclusion....193

## INTRODUCTION

In the post-9/11 world, the executive and legislative branches have drastically expanded the U.S. government's investigatory powers over its citizens through various measures including the Patriot Act,[1] which allowed the government to seize private customer records from businesses during the course of a natural security investigation, and the Foreign Intelligence Surveillance Act Amendments, which legalized the National Security Agency's domestic surveillance program.[2] Yet, as Pascal Abidor and thousands of other international travelers[3] have unexpectedly discovered in the last few years, the state can sometimes inflict an equally pernicious blow to our civil liberties simply by exercising a power that dates back to the nation's inception.[4] Society's increasing reliance on portable digital technology has allowed the government to broaden its use of the Fourth Amendment's border search doctrine, which often allows agents at our country's international borders to search travelers' belongings to a nearly unlimited extent without particularized suspicion.[5]

In May 2010, Abidor, a dual citizen of the United States and France, was crossing the U.S.-Canada border in an Amtrak train when authorities stopped him for routine questioning at a standard checkpoint.[6] Customs and Border Protection (CBP) officers discovered after several questions that Abidor was an Islamic Studies graduate student who had traveled to Jordan and Lebanon in

1. Charlie Savage, *House Votes to Extend Patriot Act Provisions*, N.Y. TIMES, Feb. 14, 2011, http://www.nytimes.com/2011/02/15/us/politics/15terror.html (noting that the provisions reauthorized by the U.S. House of Representatives "allow investigators to get 'roving wiretap' court orders allowing them to follow terrorism suspects who switch phone numbers or providers; to get orders allowing them to seize 'any tangible things' relevant to a security investigation, like a business's customer records; and to get national-security wiretap orders against non-citizen suspects who are not connected to ‚any foreign power").
2. THE CONSTITUTION PROJECT, REPORT ON THE FISA AMENDMENTS ACT OF 2008, at 1 (2012), http://constitutionproject.org/pdf/fisaamendmentsactreport_9612.pdf ("The FAA [FISA Amendments Act] vastly increased the government's powers to conduct surveillance of international communications without individualized judicial review and severely limited the scope of review performed by the FISC [Foreign Intelligence Surveillance Court] when the court's approval is actually required.").
3. *See* Complaint for Declaratory and Injunctive Relief at 1, Abidor v. Napolitano, No. CV 10-4059 (E.D.N.Y. filed Sept. 7, 2010), 2010 WL 3477769 (alleging that the government searched the electronic devices of over 6500 travelers at the international border between October 2008 and June 2010).
4. *See* Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43 (giving customs officials "full power and authority" to enter and search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed").
5. United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004).
6. Complaint for Declaratory and Injunctive Relief, *supra* note 3, at 8.

the past year.[7] Concluding that further inspection was necessary, a CBP officer removed Abidor's laptop computer from his bag, browsed the files, and noticed images, which Abidor claimed to have downloaded for research, of Hamas and Hezbollah rallies.[8] CBP questioned Abidor for three hours before releasing him, but agents kept his computer and external hard drive.[9]

CBP did not return Abidor's laptop for eleven days.[10] After receiving his laptop, Abidor allegedly discovered from his browsing history that federal agents viewed personal photos, transcripts of chats with his girlfriend, copies of emails, class notes, his tax returns, and his graduate school transcript.[11] Moreover, he alleges that CBP transmitted his files to other agencies and retained copies of those files.[12] In September 2010, the American Civil Liberties Union filed suit on behalf of Abidor and others against the Department of Homeland Security (DHS), CBP's parent agency, for allegedly violating the plaintiffs' rights through the prolonged search and seizure of their electronic devices without reasonable suspicion.[13] The case is currently pending in federal district court.[14]

The border search doctrine, which has existed since nearly the country's birth, exempts government searches of travelers' belongings from the traditional provisions of the Fourth Amendment.[15] The U.S. Supreme Court has justified this exemption by reasoning that the "[g]overnment's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[16] In particular, the Court has reasoned that border searches are important tools in "regulat[ing] the collection of duties and . . . prevent[ing] the introduction of contraband" into the United States.[17] Therefore, the executive has "plenary authority to conduct routine searches and seizures at the border."[18]

As Abidor and many others have discovered, the government has controversially begun to use the border search doctrine as authority for conducting

7. *Id.*
8. *See id.* at 8–9.
9. *Id.* at 10–11.
10. *Id.* at 10–12.
11. *Id.* at 12. Abidor's complaint, however, does not allege that forensic software was used to search his computer.
12. *Id.* at 13.
13. *Id.* at 1; Abidor v. Napolitano*: ACLU Challenges Suspicionless Laptop Border Search Policy*, AM. CIV. LIBERTIES UNION, http://www.aclu.org/free-speech-technology-and-liberty/abidor-v-napolitano (last visited Oct. 27, 2013).
14. David Kravets, *DHS Watchdog OKs 'Suspicionless' Seizure of Electronic Devices Along Border*, WIRED (Feb. 8, 2013, 1:20 PM), http://www.wired.com/threatlevel/2013/02/electronics-border-seizures.
15. *See* United States v. Ramsey, 431 U.S. 606, 617 (1977).
16. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).
17. *Id.* at 153 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985)).
18. *Id.*

suspicionless searches of international travelers' portable electronic devices.[19] These inspections are often intended to locate evidence of crimes such as child pornography[20] or terrorist activity.[21] In fact, CBP has statutory authority to use border searches to check for evidence of violations of the more than 400 laws that it is charged with enforcing.[22] Moreover, there are few meaningful restrictions on the extent of these suspicionless searches. For one, there are no statutory or agency limits on how extensively agents can probe an electronic device's memory.[23] Additionally, there are no restrictions on what type of personal information the government can view on the searched device[24] There are also no hard caps on how long the inspection can take—a few searches have taken as long as several months—and no requirement that the government return a seized device in a reasonable time and continue its search on a copy of the hard drive.[25] Under current legal precedent in the vast majority of the country, the government could possibly even confiscate and search the laptops and cell phones of every traveler disembarking from an international flight without specifying when the property would be returned or what legal violation was suspected.[26] Consequently, many judges,[27] elected representatives,[28] and legal commentators[29] have advocated for restrictions on the government's ability to conduct border searches of personal electronic devices.

This Comment aims to resolve the controversy surrounding the legality of suspicionless digital border searches by marrying a respect for the most fundamental privacy rights of individual travelers with the law's historical treatment of border searches of nonelectronic objects and of other types of suspicionless searches. Traditionally, the Fourth Amendment's requirement that all searches

19. Kravets, *supra* note 14.
20. *See, e.g.*, United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008) (holding that evidence of child pornography collected pursuant to a warrantless, suspicionless border search was admissible).
21. *See, e.g.*, *supra* notes 6–13 and accompanying text.
22. *See CBP, HSI Discover Narcotics Smuggling Ventures*, U.S. CUSTOMS & BORDER PATROL (May 15, 2013), http://www.cbp.gov/xp/cgov/newsroom/news_releases/local/2013_nr/may13/05162013.xml (mentioning that the CBP "enforce[s] over 400 laws for 40 other agencies and ha[s] stopped thousands of violators of U.S. law").
23. *See infra* Part III.C.
24. *See infra* Part III.C.
25. *See infra* Part III.C.
26. See Oral Argument at 20:00, United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc) (No. 09-10139), *available at* http://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000006188, in which Judge Alex Kozinski raised this concern in his question.
27. *See, e.g.*, *Cotterman*, 709 F.3d 952 (imposing limits on suspicionless digital border searches).
28. See *infra* Part III.D, which describes legislative efforts to curb border searches of portable electronic devices.
29. *See, e.g.*, *supra* note 13 and accompanying text (demonstrating that the American Civil Liberties Union has played a large role in challenging suspicionless digital border searches).

and seizures be reasonable has led courts to require a warrant or probable cause for most inspections.[30] Certain searches that serve limited purposes in particular settings, such as a frisk of a suspect to check for weapons, are permitted on a lower standard of reasonable suspicion.[31] Moreover, some searches, such as airport luggage scans, employee drug tests, and DUI checkpoints, have been permitted even without any suspicion under the Supreme Court's special needs doctrine.[32] Under a special needs analysis, a court will allow a search that (1) fulfills a special government need that is distinct from one of ordinary law enforcement and (2) is reasonable on balance.[33] While courts differ on the legality of suspicionless digital border searches, all have treated these inspections as separate entities from nondigital searches.[34] Breaking with the courts, this Comment argues that border searches of personal electronic devices ought to be viewed as a close relative of special needs searches because of the unique purpose of these searches and the challenges of conducting inspections at the border under ordinary Fourth Amendment requirements.[35]

Even within the special needs doctrine, however, the level of suspicion that a court requires for a search to be constitutional depends on the search's impact on privacy interests. For example, the Supreme Court treats both searches of schoolchildren's bags for drugs and drug tests of student athletes as special needs searches. But searches of schoolchildren's bags require particularized suspicion while drug tests for student athletes require no suspicion whatsoever. The difference is that student athletes have a lesser expectation of privacy than schoolchildren in general.[36] Thus, while the special needs classification is a useful heuristic for justifying lower-than-normal Fourth Amendment requirements for border searches, it does not fully answer the question of whether border searches of laptops and smart phones should require *any* suspicion. Rather, even after a search has been determined to fulfill a special need, courts weigh the govern-

30. *See, e.g.*, *Warrantless Searches and Seizures*, 40. GEO. L.J. ANN. REV. CRIM. PROC. 44, 44–45 (2011).
31. *See* Terry v. Ohio, 392 U.S. 1, 30 (1968).
32. *See, e.g.*, Chandler v. Miller, 520 U.S. 305, 323 (1997) ("[W]here the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable'—for example, searches now routine at airports and at entrances to courts and other official buildings."); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990) (upholding the use of DUI checkpoints); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989) (upholding suspicionless drug testing of government employees).
33. *See, e.g.*, *Warrantless Searches and Seizures*, *supra* note 30, at 134–35.
34. *See infra* Parts II.B–II.C.
35. *See infra* Part IV.
36. *Compare* New Jersey v. T.L.O., 469 U.S. 325, 346 (1985) (concluding that a search of a student's bag for drugs in a public school was justified on reasonable suspicion), *with* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664–65 (1995) (holding that no suspicion was required to drug test student athletes).

ment interest in the search against the expected harm to the individual's Fourth Amendment rights. At the final step of this analysis, courts require greater levels of suspicion for those searches in which the balance of interests strongly favors the individual.[37]

Courts have nearly always permitted conventional searches of nonelectronic objects without any particularized suspicion.[38] This Comment does not seek to challenge this premise. Therefore, searches of computers and other electronic devices should be subjected to greater scrutiny only if these inspections inflict significantly greater harms to an individual's Fourth Amendment interests than searches of nonelectronic objects.[39] While rejecting the argument that the large storage capacity of laptops and their capability to store personal information makes laptops completely distinct from any nondigital object,[40] this Comment argues that digital border searches deserve stricter regulation than more conventional searches for several reasons. First, while sensitive personal information may be jeopardized even in a conventional search, the particular mechanics of digital searches and the frequency with which people store personal information on their electronic devices makes the discovery of private information highly likely in these types of inspections.[41] Additionally, the amount of personal information available to government agents creates ample opportunities for them to abuse their powers and turn these searches into dragnets meant to detect any type of illegal activity.[42]

Second, unlike searches of physical containers, extensive computer searches can uncover not only the user's current files but also information that the individual may have browsed or deleted in the past. Since individuals sometimes have a limited ability to restrict what information is preserved in a device's memory, a traveler may not have the option of preemptively ensuring that sensitive data will not be disclosed if he or she is the subject of a border search.[43] Third, because many travelers use cloud computing to store personal information on remote servers, accessible through their portable devices, digital border searches can further intrude on their privacy by allowing the government to view information that the these travelers never actually transported across the bor-

37. *See infra* note 86 and accompanying text.
38. *See* United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008) (citing cases upholding suspicionless searches of travelers' luggage, purses, pockets, and graphic materials).
39. *See infra* Part III.A.
40. *See infra* Part III.A.
41. *See infra* Part III.A.
42. *See infra* Part III.A.
43. *See infra* Part III.B.

der.[44] Lastly, the lack of forensic software to search computers at many border checkpoints and the extensive amount of information that agents have to comb through means that a traveler's electronic device is more likely than a physical container to be detained by agents and removed from his possession for further inspection.[45] Thus, additional limits on digital border searches of travelers' property are warranted.

Although CBP and Immigrations and Customs Enforcement (ICE) released directives in 2009 to establish guidelines for border searches of electronic devices, the directives nonetheless preserved agents' power to conduct extended searches of nearly unlimited scope without reasonable suspicion.[46] Moreover, legislative efforts to establish more vigorous safeguards against these types of inspections have stalled in the U.S. Congress.[47] Consequently, major reform will likely have to occur through the courts, which in the past have imposed additional safeguards against border searches of the person[48] and border searches that destroy property.[49] Unfortunately, courts ruling on this issue have either upheld the legality of suspicionless digital border searches or required reasonable suspicion for particular searches without providing a broad, animating principle that can instruct courts in future cases.[50] Because searches of portable electronic devices can vary so greatly from one another, an ad hoc approach to each case, with no guidance other than previous rulings, will provide neither clarity nor an effective bulwark against highly intrusive digital border searches.[51]

This Comment proposes that courts provide such an organizing principle by treating digital border searches like other special needs searches. Through the introduction of a unique model for evaluating the propriety of suspicionless border searches of electronic storage devices, this Comment argues that courts should adopt a special needs–style balancing test for digital border searches that not only weighs the intrusiveness of the search but also whether a distinct gov-

44. *See infra* Part III.B.
45. *See infra* Part III.B.
46. *See infra* Part III.C.
47. *See infra* Part III.D.
48. *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) (holding that the detention of the defendant at an international airport for over one day was justified upon the government showing reasonable suspicion that the defendant was transporting drugs in her alimentary canal).
49. *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 154 & n.2 (2004) (citing searches involving exploratory drilling in reasoning that searches that destroy property may require a heightened level of suspicion).
50. *See infra* Part II.B.
51. *See infra* Part II.C.

ernment need is being served at the border.[52] Additionally, instead of arbitrarily deciding what constitutes an intrusive search, courts ought to consider three factors that the Supreme Court has considered to be relevant to Fourth Amendment interests in other special needs cases: the nature and amount of the information searched, the duration of the search, and the presence or absence of an extended detention of the property.[53] The proposed test differs slightly from the ordinary special needs test so that a court would not be forced to contradict itself by prohibiting suspicionless digital searches that investigate violations of certain laws that, under the traditional border search doctrine, can be permissibly investigated through suspicionless conventional searches.

This model will have three benefits. First, it will ultimately result in greater protection for international travelers' privacy interests in their electronic devices.[54] Second, it will provide animating principles to help resolve much of the legal uncertainty surrounding suspicionless digital border searches that stems from the widely varying decisions from lower courts.[55] Last, it will help transform the digital border search doctrine from a Fourth Amendment anomaly to one that is far more consistent with the limited instances in which courts have allowed law enforcement to deviate from the amendment's ordinary requirements.[56]

This Comment proceeds as follows: Part I provides a brief background on ordinary Fourth Amendment jurisprudence, including the special needs doctrine that exempts certain searches and seizures from ordinary warrant and probable cause requirements. Part II then introduces the law's historical treatment of border searches. First, this Part provides a brief history of the doctrine's origin, justification, and scope. This Part then discusses the current maze of uncertainty, which one judge has referred to as a "legal bouillabaisse,"[57] surrounding the legality of suspicionless border searches of personal electronic de-

52. While previous literature on the border search doctrine has argued that border searches are analogous to special needs searches, *see, e.g.*, Victoria Wilson, Note, *Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders From Bombs, Drugs, and the Pictures From Your Vacation*, 65 U. MIAMI L. REV. 999, 1016–17 (2011), the model proposed in this Comment for evaluating the constitutionality of digital border searches is unique and is the creation of the author.

53. *See infra* Part IV.A.2.

54. Greater protections will result because of the model's incorporation of three factors that the individual can use to demonstrate harms to his or her Fourth Amendment interests. *See infra* Part IV.A.2.

55. The animating principles that future courts can use for guidance are the test for determining whether the digital border search is meeting a special need, as outlined *infra* Part IV.A, and the three-factor test to calculate the harms to the individual's interest, as outlined *infra* Part IV.A.

56. Treating digital border searches more like special needs searches, as outlined *infra* Part IV.A., will result in added consistency.

57. United States v. Cotterman, 709 F.3d 952, 981 (9th Cir. 2013) (en banc) (Smith, J., dissenting).

vices. This Part then concludes with a critique of the way courts have framed the issue and argues that border searches are better classified as a close relative of a special needs search. Part III looks at the aspects of computer border searches that make such searches more intrusive on individuals' Fourth Amendment interests than conventional border searches and addresses counterarguments from both sides of the debate. It then evaluates how current federal policy regarding computer border searches impacts the vulnerabilities identified earlier and briefly notes unsuccessful legislative attempts to protect the privacy of international travelers. Part IV then proposes the special needs–style model for evaluating the permissibility of suspicionless digital border searches. This Part also addresses potential counterarguments, both from those who would uniformly subject all digital border searches to a reasonable suspicion requirement and from those who would categorically exempt all such inspections from the requirement.

## I. THE HISTORY AND JUSTIFICATION OF SUSPICIONLESS SEARCHES

### A. Ordinary Fourth Amendment Jurisprudence

The Fourth Amendment to the U.S. Constitution guarantees individuals the "right . . . to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government.[58] The Supreme Court has held that a reasonable search or seizure must be both "justified at its inception" and "reasonably related in scope to the circumstances which justified the interference in the first place."[59] In order for a search to be justified at its inception under the Fourth Amendment, the "nature and extent of the governmental interests" in conducting the search must outweigh the "nature and quality of the intrusion on individual rights" that would occur if the government conducted the search.[60] This first element of the test essentially discerns whether, ex ante, the search can be justified in theory. The second element of the reasonableness test requires that the search be "reasonably designed" to achieve the

58. U.S. CONST. amend. IV.
59. Terry v. Ohio, 392 U.S. 1, 19–20 (1968).
60. *See id.* at 23–30 (reasoning that a police officer's interest in protecting himself by searching the petitioner during an investigative stop to ensure that the petitioner was not armed, coupled with his reasonable belief that the petitioner was armed, outweighed the intrusion on the petitioner's personal security resulting from a patdown of the petitioner's outer clothing).

legitimate governmental ends that factor into the first element's balancing test.[61] This element evaluates whether, ex post, there was a reasonable fit between the ends and means of the search.

Generally, this Fourth Amendment rubric has required that a government search or seizure be based on a warrant or probable cause of a legal violation that the search aims to investigate.[62] Courts have also recognized, however, the government's power to conduct certain limited-scope searches in particular settings upon a lesser standard of "reasonable suspicion."[63] This standard is met when the government can "point to specific and articulable facts, which, taken together with rational inferences from those facts, reasonably warrant th[e] intrusion."[64] Moreover, these facts and inferences must be connected to the individual suspect. Hence, the "reasonable suspicion" requirement is often referred to as "individualized" or "particularized" suspicion.[65] In addition to certain border searches of the person, searches that the Supreme Court has allowed on "reasonable suspicion" include patdowns for weapons searches during investigative stops[66] or traffic stops,[67] limited vehicle searches for weapons during traffic stops,[68] and school officials' searches of students' bags for drugs.[69]

### B. Permissible Suspicionless Searches

The Supreme Court has also permitted certain Fourth Amendment searches to occur under no individualized suspicion whatsoever. Such searches, which include searches of passengers' luggage at airports,[70] drug testing of gov-

61. *Id.* at 29 ("[E]vidence may not be introduced if it was discovered by means of a seizure and search which were not reasonably related in scope to the justification for their initiation." (citing Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring)).
62. *See, e.g.*, *Warrantless Searches and Seizures*, *supra* note 30, at 44–45.
63. *Id.* at 45 (quoting *Terry*, 392 U.S. at 20–21) (internal quotation marks omitted).
64. *Id.* (alteration in original) (quoting *Terry*, 392 U.S. at 21) (internal quotation marks omitted).
65. *See Terry*, 392 U.S. at 27 ("[I]n determining whether the officer acted reasonably in such circumstances, due weight must be given, not to his inchoate and unparticularized suspicion or 'hunch,' but to the specific reasonable inferences . . . ."); Alexander A. Reinert, *Revisiting "Special Needs" Theory Via Airport Searches*, 106 NW. U. L. REV. 1513, 1522 n.48 (2012) ("The standard of individualized suspicion adopted by the *Terry* Court has come to be known as 'reasonable suspicion.'").
66. *See Terry*, 392 U.S. at 30.
67. *See* Pennsylvania v. Mimms, 434 U.S. 106, 111–12 (1977).
68. *See* Michigan v. Long, 463 U.S. 1032, 1051 (1983).
69. *See* New Jersey v. T.L.O., 469 U.S. 325, 346 (1985).
70. *See* United States v. Aukai, 497 F.3d 955, 958–60 (9th Cir. 2007) (en banc); *see also* Chandler v. Miller, 520 U.S. 305, 323 (1997) ("[W]here the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable'—for example, searches now routine at airports and at entrances to courts and other official buildings.").

ernment employees[71] and student athletes,[72] highway sobriety checkpoints,[73] and highway roadblocks to intercept fleeing criminals,[74] have generally been justified under the Fourth Amendment's special needs doctrine.[75] This doctrine, when applied by the Court, lowers the level of suspicion required to render a government search reasonable.[76] A special needs analysis, which determines whether the search is justified at its inception, has two steps.[77] First, the court must determine if the search addresses a special need—meaning that it combats a current and vital problem that goes beyond an ordinary law enforcement need to detect criminal wrongdoing[78]—that would be largely frustrated if the Fourth Amendment's ordinary protections applied.[79] In addition, the government need must be especially significant to the location of the search.[80] For example, on a public highway, a motorist who is breaking the law by driving while intoxicated is particularly dangerous because he jeopardizes the security of everyone else on the road. Without any investigation, police may be able to find proof of a driver's violation of this law only once the driver has caused an accident. Therefore, the government interest in identifying drunk drivers on a highway is a special need that could not be effectively addressed if the government needed probable cause before pulling someone over on suspicion of drunk driving.[81] By contrast,

71. *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 634 (1989).
72. *See* Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls, 536 U.S. 822, 836 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664–65 (1995).
73. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).
74. *See* Illinois v. Lidster, 540 U.S. 419, 427–28 (2004).
75. *See* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 3.9 (3d ed. 2007). LaFave states that the court decisions discussed in this section, including the cases cited in *supra* notes 71–74, "are typically justified in terms of what it is that necessitates deviation from the usual Fourth Amendment requirements, usually described in terms of some 'special need' distinct from ordinary law enforcement." *Id.* § 3.9(a).
76. *See id.*
77. *Warrantless Searches and Seizures*, *supra* note 30, at 134–35.
78. *Id.* For examples of cases in which the government search fulfilled a special need, see the cases cited in *supra* notes 71–74. For an example of a case in which the government search merely fulfilled an ordinary law enforcement goal, see *Ferguson v. City of Charleston*, 532 U.S. 67, 85–86 (2001), holding a hospital's drug testing of pregnant women unconstitutional because the primary purpose was to generate evidence of illegal drug use for law enforcement prosecution.
79. New Jersey v. T.L.O., 469 U.S. 325, 340 (1985) (holding that the unique need of maintaining order in school justified a search of the defendant's purse on reasonable suspicion of drug possession because the Fourth Amendment's warrant requirement would "frustrate the governmental purpose behind the search" (quoting Camara v. Mun. Court, 387 U.S. 523, 532–33 (1967))).
80. *See, e.g.*, City of Indianapolis v. Edmond, 531 U.S. 32, 41–48 (2000) (reasoning that the suspicionless DUI checkpoints in *Sitz* were upheld due to their close connection to the special need of ensuring highway safety, whereas the general narcotics interdiction checkpoints in the present case could not "be rationalized in terms of a highway safety concern similar to that present in *Sitz*").
81. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

while motorists who are transporting illegal drugs are also violating the law, they do not necessarily pose a greater threat to the safety of the road than others. Thus, the apprehension of narcotics traffickers on a public highway is not a special need but only an ordinary law enforcement goal, and a checkpoint designed to detect drug smugglers rather than drunk drivers would not fulfill a special need.[82]

If the presiding court concludes that the search fulfills a special need, it then engages in a reasonableness balancing test between the government and individual interests at hand.[83] In estimating the state's interests, the court considers the severity of the problem that the search addresses[84] and the search's likely effectiveness in mitigating those harms.[85] Occasionally, courts have concluded that even if a search fulfills a special need, it is nonetheless too intrusive to comport with the Fourth Amendment absent higher levels of suspicion.[86] But if the search is deemed reasonable on balance, the inspection passes the special needs test. The court will then conclude that the search complies with the Fourth Amendment.[87]

82. *See Edmond*, 531 U.S. at 41–43 (distinguishing the DUI checkpoints in *Sitz*, which served a special need, from suspicionless highway checkpoints designed to detect the possession and transport of narcotics, which only served "general crime control ends," since "[o]nly with respect to a smaller class of offenses . . . is society confronted with the type of immediate, vehicle-bound threat to life and limb that the sobriety checkpoint in *Sitz* was designed to eliminate").

83. *See Warrantless Searches and Seizures*, *supra* note 30, at 134–35.

84. For examples of the Supreme Court's estimation of the severity of the problem addressed by a special needs search, compare *Vernonia School District 47J v. Acton*, 515 U.S. 646, 661–64 (1995), which concludes that the government interests were high because of the high percentage of athletes at the school using drugs and because of the danger of mixing drug use with physical activity, with *Chandler v. Miller*, 520 U.S. 305, 318–19 (1997), which concludes that the goal of deterring drug use by state elected officials was not "sufficiently vital" to justify bypassing ordinary Fourth Amendment requirements because "[n]othing in the record hint[ed] that the hazards . . . are real and not simply hypothetical."

85. *Compare Vernonia Sch. Dist. 47J*, 515 U.S. at 663–64 (considering "the efficacy of [the] means for addressing the problem" and concluding that student athlete drug use was "effectively addressed" through testing to ensure that athletes did not use drugs), *with Chandler*, 520 U.S. at 319–20 (reasoning that the scheduled drug tests would be ineffective at deterring drug use because the individuals could schedule the tests up to thirty days in advance and intentionally abstain for a small period of time prior to the test and then resume drug use after passing the test).

86. *See* Delaware v. Prouse, 440 U.S. 648, 663 (1979) (holding that the government interest in ensuring highway safety did not justify random, suspicionless stops of motorists to check for licenses and registration); Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 356–57 (8th Cir. 2004) (holding that the suspicionless search of public school students' belongings to check for weapons and drugs violated the Fourth Amendment); *cf.* United States v. Place, 462 U.S. 696, 709–10 (1983) (holding that, despite the strong government interest in preventing narcotics trafficking, the ninety-minute detention of the respondent's luggage was unreasonable in the absence of probable cause).

87. *See Warrantless Searches and Seizures*, *supra* note 30, at 134–35.

## II. BORDER SEARCHES

Although the Supreme Court has specifically recognized the special needs doctrine only in the last several decades,[88] the border search doctrine, which also excuses certain searches from ordinary Fourth Amendment requirements, dates back to the nation's founding period.[89] Indeed, "[i]t has always been understood that the sovereign had plenary power to control the introduction of contraband across its borders from abroad and to insure its physical security and protect its revenue by a thorough search of all persons and chattels entering the country."[90] Presently, rulings by the Supreme Court and circuit courts have established that the border search doctrine applies not only to incoming people and property at the international border but also to those that exit[91] in order to prevent the export of items such as drugs, weapons, unlicensed goods,[92] or undeclared currency.[93] Courts have also defined the border to include a "functional equivalent" of a border, which constitutes the first point within the United States where persons or property can practicably be searched after arriving from abroad[94] or the

88. *See* Jennifer E. Smiley, Comment, *Rethinking the "Special Needs" Doctrine: Suspicionless Drug Testing of High School Students and the Narrowing of Fourth Amendment Protections*, 95 NW. U. L. REV. 811, 816 (2001) ("Justice Blackmun's concurrence in *T.L.O.* first articulated the special needs doctrine." (citing New Jersey v. T.L.O., 469 U.S. 325, 351–53 (1985) (Blackmun, J., concurring))).

89. *See* Ari B. Fontecchio, Comment, *Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception That Swallows Your Laptop*, 31 CARDOZO L. REV. 231, 234 (2009) (describing the border search doctrine as a "manifestation of the special needs doctrine").

90. Jules D. Barnett, *A Report on Search and Seizure at the Border (Customs Problems)*, 1 AM. CRIM. L.Q. 36, 39 (1963).

91. United States v. Beras, 183 F.3d 22, 26 (1st Cir. 1999) (holding that the border search exception applies to outgoing travelers and noting that "[e]very other circuit to consider the issue . . . has held that the border search exception applies to outgoing as well as incoming travelers" (citing United States v. Ezeiruaku, 936 F.2d 136, 143 (3d Cir. 1991); United States v. Berisha, 925 F.2d 791, 795 (5th Cir. 1991); United States v. Udofot, 711 F.2d 831, 839–40 (8th Cir. 1983); United States v. Ajlouny, 629 F.2d 830, 834–35 (2d Cir. 1980); United States v. Stanley, 545 F.2d 661, 667 (9th Cir. 1976))).

92. *Stanley*, 545 F.2d at 667 n.8.

93. *Ezeiruaku*, 936 F.2d at 142–43 (citing United States v. Hernandez-Salazar, 813 F.2d 1126, 1138 (11th Cir. 1987)).

94. Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973) ("[A] search of the passengers and cargo of an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City would clearly be the functional equivalent of a border search."); *cf.* United States v. Gaviria, 805 F.2d 1108, 1114 (2d Cir. 1986) (holding that a search of cargo in New York, even after the cargo had initially entered the United States at Miami, where one-tenth of the property was searched, was a search at the "functional equivalent" of a border when New York was the intended final destination, the goods remained under a customs bond after entering the United States, and there was no evidence that anyone had tampered with the goods in transit). The functional equivalent doctrine also encompasses permanent checkpoints on major roads leading away from the border, even if the checkpoint is not on the border itself, if locating the checkpoint closer to the border would reduce its effectiveness and excessively interfere with traffic. *See* United States v. Martinez-Fuerte, 428

last domestic point where the person[95] or his property[96] can be searched before exiting. For example, a customs desk at an international airport is a functional equivalent of a border because it is the first point at which an international traveler and his or her luggage can be searched after entering the country. Thus, the border search doctrine applies not only to searches of people and property entering or exiting at an actual international border but also to inspections of people and property that are beginning or concluding international travel at an airport or other inspection station in the interior of the country.

The law's deferential treatment of border searches dates back to the very beginning of the United States. In 1789, the First Congress, the same body that proposed the Fourth Amendment fifty-four days later, passed the nation's first customs statute, which exempted searches of naval vessels from ordinary warrant requirements so long as officers had "reason to suspect" the ships were concealing dutiable goods.[97] Notably, this same statute also articulated that searches for a similar purpose inside buildings required a warrant.[98] Unlike ships, buildings did not carry their concealed contraband across international borders. Thus, even in the eighteenth century, border policing received especially permissive treatment from the federal government.

For the next two centuries, the government continued to maintain customs statutes exempting searches of persons and property crossing the border from the level of suspicion required for searches on the country's interior.[99] Although the Supreme Court had few opportunities to rule on the constitutionality of particular border searches, two rulings in the 1880s established that federal agents had the power to conduct warrantless searches and seizures for dutiable goods at the border[100] and in international mail.[101] Still, these early decisions did not go so far as to say that border searches were permissible without even a shade of individualized suspicion.

---

U.S. 543, 553, 562 n.15 (1976). The first port of entry where a ship docks after entering the United States from abroad, even if within the interior of the country, is also considered the functional equivalent of a border. United States v. Prince, 491 F.2d 655, 659 (5th Cir. 1974). Furthermore, when the United States has an agreement with another country for U.S. officials to conduct preclearance searches of people and property about to depart for the United States at the other country's ports, those searches are treated as equivalent to border searches. United States v. Walczak, 783 F.2d 852, 856 (9th Cir. 1986).

95. United States v. Duncan, 693 F.2d 971, 977 (9th Cir. 1982).
96. United States v. Abbouchi, 502 F.3d 850, 855–56 (9th Cir. 2007).
97. Barnett, *supra* note 90, at 39 (discussing Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43).
98. *Id.*
99. *Id.* at 40.
100. Boyd v. United States, 116 U.S. 616, 623 (1886).
101. Cotzhausen v. Nazro, 107 U.S. 215, 218–19 (1882).

In the 1970s and 1980s, however, the Supreme Court extended the government's border search powers by permitting certain suspicionless inspections. For example, in *United States v. Martinez-Fuerte*,[102] the Court upheld suspicionless highway checkpoint stops of individuals entering the United States from Mexico to detect the transportation of unauthorized immigrants.[103] Then, in *United States v. Montoya de Hernandez*,[104] the Court stated in dictum that "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant."[105] In 2004, the Court notably established that any border search of a vehicle fell into this category, when it upheld the suspicionless border search of a suspect's gas tank in *United States v. Flores-Montano*.[106]

### A. Border Searches Presently Requiring Reasonable Suspicion

Despite the government's broad powers to conduct suspicionless border searches, the Supreme Court and lower courts have generally required reasonable suspicion for searches and seizures at the border that significantly intrude on the individual's Fourth Amendment interests.[107] First, "highly intrusive" searches of the person, such as extended detentions, strip searches, or cavity searches, must clear this threshold because of their strong impact on the individual's "dignity and privacy interests."[108] Second, property searches which physically destroy or damage the property, such as searches involving exploratory drilling, are likely to be subjected to a reasonable suspicion requirement.[109] Moreover, the Supreme

102. 428 U.S. 543 (1976).
103. *Id.*
104. 473 U.S. 531 (1985).
105. *Id.* at 538.
106. 541 U.S. 149, 155 (2004).
107. *Montoya de Hernandez*, 473 U.S. at 540–41.
108. *Flores-Montano*, 541 U.S. at 152; *see also Montoya de Hernandez*, 473 U.S. at 544 (finding that reasonable suspicion that suspect was smuggling drugs in her alimentary canal justified her detention for over a day at the border); United States v. Vega-Barvo, 729 F.2d 1341, 1350 (11th Cir. 1984) (holding that reasonable suspicion that the suspect was smuggling drugs internally justified an x-ray search of the suspect's body); United States v. Guadalupe-Garza, 421 F.2d 876, 879 (9th Cir. 1970) ("'Real suspicion' justifying the initiation of a strip search is subjective suspicion supported by objective, articulable facts that would reasonably lead an experienced, prudent customs official to suspect that a particular person seeking to cross our border is concealing something on his body for the purpose of transporting it into the United States contrary to law."); Rivas v. United States, 368 F.2d 703, 711–12 (9th Cir. 1966) (holding that search of the petitioner's anal cavity at the border was justified by the "clear indication" that he was smuggling drugs in a body cavity).
109. *See Flores-Montano*, 541 U.S. at 154–55 n.2 (distinguishing the disassembly and reassembly of a fuel tank, which required no suspicion, from "potentially destructive drilling"); *see also id.* at 155–56 (noting that some searches of property are "so destructive as to require" particularized suspicion); United States v. Rivas, 157 F.3d 364, 367–68 (5th Cir. 1998) (holding that drilling into a metal

Court in *Flores-Montano* hinted that this standard may apply to any border search carried out in a "particularly offensive manner."[110] Nonetheless, the Court has never held that reasonable suspicion is required for a nondestructive property search at the border.

### B. Courts' Varying Treatment of Border Searches of Personal Electronic Devices

Despite the lack of Supreme Court precedent requiring any level of suspicion for border searches of property, federal courts have varied greatly in their conclusions about the legality of suspicionless border searches of electronic property such as laptop computers. Moreover, the courts' rationales for these holdings have very little in common.

For example, in *United States v. Ickes*,[111] the Fourth Circuit in 2005 upheld a border search of a suspect's laptop computer and portable diskettes that revealed evidence of child pornography.[112] Though noting that these searches will often be supported by reasonable suspicion, the court reasoned that this requirement should not be "enthron[ed] . . . as a matter of constitutional law" since "[t]he essence of border search doctrine is a reliance upon the trained observations and judgments of customs officials, rather than upon constitutional requirements."[113] In addition to the policy argument that law enforcement officials, rather than courts, know best when a search is justifiable, the court also made a basic constitutional argument. Comparing the government's "overriding interest in . . . prevent[ing] 'the introduction of contraband into this country'" against the individual's "substantially lessened" expectation of privacy at the border, the court concluded that digital searches such as the one in the present case were reasonable on balance.[114] Thus, even had it concluded unambiguously that no basis for particularized suspicion existed, the Fourth Circuit's reasoning demonstrates that it would likely have upheld the constitutionality of the search of the suspect's computer and diskettes.

---

trailer was a nonroutine border search that was unreasonable because of lack of reasonable suspicion); United States v. Robles, 45 F.3d 1, 5–6 (1st Cir. 1995) (holding that drilling into a metal cylinder was a nonroutine search that was justified by the government's reasonable suspicion).

110. *Flores-Montano*, 541 U.S. at 154–55 n.2 (citing United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977)).

111. 393 F.3d 501 (4th Cir. 2005).

112. *Id.* at 507–08.

113. *Id.* at 507.

114. *Id.* at 506 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985)).

The Ninth Circuit's decision in *United States v. Arnold*[115] in 2008 largely mimicked the reasoning of the *Ickes* court. In *Arnold*, the court held that reasonable suspicion was not required when CBP agents browsed two desktop folders on a defendant's laptop, discovered a photo of two nude women, and then found numerous images of child pornography while manually browsing the computer over the next several hours.[116] The court reasoned that the Supreme Court's upholding of a suspicionless border search of a gas tank in *United States v. Flores-Montano*[117] meant that reasonable suspicion was not required for any property searches at the border. Essentially, the court decided that such searches could never be intrusive enough to require reasonable suspicion, since "a piece of property . . . does not implicate the same 'dignity and privacy' concerns as 'highly intrusive searches of the person.'"[118] To further buttress this point, the court also described laptop searches as indistinguishable from searches of closed containers and luggage,[119] which the Supreme Court has permitted without any suspicion.[120] Thus, like the Fourth Circuit in *Ickes*, the *Arnold* court effectively concluded that the balance of interests in a border search of property would always favor the government.

A Massachusetts federal district court's holding in 2012 in *House v. Napolitano*[121] established a jurisdictional split by treating digital border searches differently from the *Ickes* and *Arnold* courts. In *House*, agents stopped the suspect when he disembarked from an international flight at Chicago's O'Hare International Airport, allegedly because of his connections to WikiLeaks informant Bradley Manning.[122] After the suspect refused to provide the password to his laptop, agents confiscated the computer as well as a USB flash drive, video camera, and cellular phone.[123] The district court first held that the search and seizure at the airport did not require any reasonable suspicion because, like the

115. 533 F.3d 1003 (9th Cir. 2008).
116. *Id.* at 1005–06, 1008.
117. 541 U.S. 149, 152 (2004) ("But the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles. Complex balancing tests to determine what is a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person, have no place in border searches of vehicles.").
118. *Arnold*, 533 F.3d at 1008 (quoting *Flores-Montano*, 541 U.S. at 152).
119. *Id.* at 1007 (citing cases upholding suspicionless searches of travelers' luggage, purses, pockets, and graphic materials).
120. *Id.* at 1009 (citing United States v. Ross, 456 U.S. 798, 823 (1982)).
121. No. 11-10852-DJC, 2012 WL 1038816 (D. Mass. Mar. 28, 2012).
122. *Id.* at *2–3.
123. *Id.* at *3.

*Arnold* court, it viewed laptop searches, like all property searches, as significantly less intrusive than searches of the person.[124]

Nevertheless, the court denied the government's motion to dismiss the suspect's suit and ruled that the Fourth Amendment claim would be resolved based on "whether the 49-day detention of House's electronic devices was reasonably related in scope to the circumstances that may have justified it at the border."[125] Thus, the holding implies that the search in question, though permissible at the onset, may violate the second prong of the Fourth Amendment's reasonableness test by not being "reasonably related in scope to the circumstances which justified the interference."[126] Yet, by only ruling that the means of the search may not have reasonably fit the ends, the *House* court failed to elaborate on how extensive a suspicionless computer border search can be before the government could not justify the ends ex ante. Because agency directives already require CBP and ICE agents to confine the scope of a border search to the purpose for the original search, this precedent is unlikely to aid most people targeted by digital border searches.[127]

Despite its highly deferential holding in *Arnold*, the Ninth Circuit further complicated the existing caselaw in March 2013 when it concluded in *United States v. Cotterman*[128] that reasonable suspicion *was* required for a comprehensive forensic search of a suspect's laptop.[129] In this inspection, CBP agents detained the suspect's computer at the U.S.-Mexico border after a background check revealed that he was a sex offender.[130] The officers transferred the computer inland to a lab in Tucson, Arizona. Over the next two days, analysts used forensic software to make copies of the computer hard drives and to search the copies, and eventually found seventy-five images of child pornography within

124. *Id.* at *7.
125. *Id.* at *9.
126. Terry v. Ohio, 392 U.S. 1, 20 (1968).
127. *See infra* Part III.C. Assuming that CBP and ICE agents follow their directives, it is unlikely that most individuals challenging such searches would be the victims of a search in which the prolonged detention had no connection at all to CBP's or ICE's need to investigate the violation of a law that the agency is in charge of enforcing. Additionally, the importance of preventing the government from abusing its investigatory powers by confining the scope of a search under the Fourth Amendment to the original circumstances justifying the search is relatively obvious. Thus, this Comment focuses only on whether the prolonged detention of electronic property can render the search unreasonable at its inception. *See infra* Part IV.
128. 709 F.3d 952 (9th Cir. 2013) (en banc).
129. *Id.* at 967–68.
130. *Id.* at 957–58.

the laptop's unallocated space.[131] In March 2013, the Ninth Circuit, sitting en banc, concluded that although the authorities' transfer of the suspect's computer to a site away from the border was not relevant to the Fourth Amendment analysis, the forensic software used in the search distinguished the inspection from the one in *Arnold* and made it sufficiently intrusive to require reasonable suspicion.[132] Nonetheless, this conclusion appears to be incompatible with the rationale of *Ickes* and *Arnold* that property searches at the border are *never* intrusive enough to require reasonable suspicion.[133] Moreover, *Cotterman*'s ruling that reasonable suspicion is required for a digital border search also differs from the ruling in *House* that such an inspection may be justified at the onset but eventually would reach an impermissible scope. Thus, the Ninth Circuit in *Cotterman* established a three-way split between federal courts regarding the permissibility of suspicionless digital border searches.

### C. Consequences of the Interjurisdictional Split

The three-way divergence in rulings on suspicionless border searches of portable electronic devices leaves three negative consequences for any courts that confront the issue. First, and most obviously, other courts lack clear guidance on whether suspicionless searches of laptops and similar devices should ever be treated differently from suspicionless searches of physical property such as luggage or vehicles, which have almost always been permissible.

Second, even if a court decides that digital searches may occasionally require reasonable suspicion, the limited scope of the *Cotterman* and *House* rulings leaves the court with no authority or animating principle to rely on if it confronts a case in which the search is notably different from the searches in the precedent cases. For example, what if the government begins by manually perusing the suspect's computer files, as it did in the *Arnold* case, but then detains the computer to manually browse the machine, without the use of additional forensic software, for several days, rather than several hours? Or, what if the government accesses information that is ordinarily password protected without using forensic search programs because it correctly guesses the password or because the suspect saved his password? Since the *Cotterman* decision hinged on

131. *Id.* at 958. "Unallocated space" refers to space on a hard drive where a computer stores information that the user has previously deleted or information from websites the user has previously visited. *Id.* at 958 n.5.

132. *Id.* at 962–63.

133. United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008).

the use of forensic software to trawl the suspect's computer, a court confronting an extensive manual search would find *Cotterman* inapposite.[134]

Third, although the majority of laws enforced by CBP and ICE involve identifying the smuggling of prohibited contraband (such as drugs or child pornography) or detecting behavior that is especially pernicious when the suspect is in the midst of crossing an international border (such as transporting large amounts of currency),[135] none of the existing holdings provide any principle that prevents border agents from using the border search doctrine as a carte blanche to search for a violation of any other law.[136] This omission is significant because, in general, searches conducted without a warrant or probable cause and without a suspect's consent or the object's presence in plain view are permissible only when confined to particular circumstances. For example, in any special needs search, the government end must be a special need with particular relevance at the setting of the search, rather than a general need to enforce the law.[137] As another example, in a stop-and-frisk search, when an officer reasonably suspects that the suspect may be "armed and dangerous," the officer must confine the search to one designed to discover weapons.[138] Similarly, in a search incident to arrest, officers are only allowed to search the area within a suspect's immediate control for weapons or destructible evidence.[139] Yet even in *House* "agents did not ask House any questions related to border control, customs, trade, immigration or terrorism, and at no point did the agents suggest that House had engaged in any illegal activity or that his computer contained any illegal material."[140] The court did not attempt to cabin the reasons for which the government could initiate a suspicionless inspection of the suspect's computer.[141] Thus, courts' unwillingness to confine border searches to the purposes for which the border search doctrine exists illustrates the doctrine's incompatibility

134. *See* Orin Kerr, *What Is the Ninth Circuit's Standard for Border Searches Under* United States v. Cotterman*?*, VOLOKH CONSPIRACY (Mar. 11, 2013, 3:12 PM), http://www.volokh.com/2013/03/11/what-is-the-ninth-circuits-standard-for-border-searches-under-united-states-v-cotterman (raising such questions in response to the *Cotterman* decision).

135. *See infra* Part IV.A.1.

136. *See* Kravets, *supra* note 14 (expressing the fear "that travelers along the nation's borders may have their electronics seized and the contents of those devices examined for any reason whatsoever").

137. *See supra* Part I.B.

138. Terry v. Ohio, 392 U.S. 1, 30 (1968).

139. Chimel v. California, 395 U.S. 752, 762–63 (1969).

140. House v. Napolitano, No. 11-10852-DJC, 2012 WL 1038816, at *4 (D. Mass. Mar. 28, 2012).

141. *Id.*

with the Fourth Amendment's general treatment of searches that are unsupported by a warrant or probable cause.[142]

### D. Framing Digital Border Searches as Special Needs Searches

Courts must begin resolving the legal uncertainty regarding suspicionless digital border searches by treating these searches not as a unique entity under the Fourth Amendment but instead as a close relative of a special needs search.[143] Logically, there is no reason why border searches are distinct from searches that have been justified under the special needs doctrine.[144] As with special needs searches of schoolchildren,[145] airport searches,[146] and highway searches,[147] border searches typically address a special governmental need at the setting of the search—for example, the prevention of the transport of illegal contraband into the United States. Moreover, as with all these searches, application of the Fourth Amendment's ordinary protections to border searches would frustrate the government's purpose. Just as the state could not ensure airplane safety if it needed a warrant or probable cause before scanning luggage for explosives, the state could not effectively prevent contraband from entering the country if it needed a warrant or probable cause before inspecting someone's vehicle or portable hard drive.[148] Thus, since border searches fit the Supreme Court's definition of special needs searches, they ought to be treated similarly.

The doctrinal obstacle to treating digital border searches exactly like special needs searches is that the Supreme Court has never treated conventional border searches in this manner. Instead of considering whether a border search is related to a law that the government has a particular need to enforce at the border, the Court has reasoned that border searches "are reasonable simply by

142. *See* Wilson, *supra* note 52, at 1017 ("[U]nlike 'special needs' searches, the balancing test at the border does not seem to be limited, in practice, to searches that are separate from general law enforcement, and searches at the border are not limited to the justifiable scope of the justified intrusion.").

143. *See id.* at 1016–17.

144. *See* 5 WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10.1 n.1 (5th ed. 2012) (classifying all searches including both border searches and special needs searches like school searches as "part of a larger field, commonly referred to as 'administrative searches'").

145. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995); New Jersey v. T.L.O, 469 U.S. 325 (1985).

146. *See* United States v. Place, 462 U.S. 696 (1983).

147. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

148. *See* YULE KIM, CONG. RESEARCH SERV., RL31826, PROTECTING THE U.S. PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT (2009) (implying that a border search is a "situation[] that render[s] obtaining a warrant impractical or against the public's interest").

virtue of the fact that they occur at the border."[149] Similarly, rather than weighing whether the government interest outweighs the individual's, as special needs test would do, the Court has concluded that "[c]omplex balancing tests . . . have no place" in determining the constitutionality of border searches of conventional property such as vehicles.[150] Therefore, transmuting the entire border search doctrine into the special needs doctrine, though it may be logical, would clash with longstanding precedent.

Rather than overturn existing Supreme Court precedent, this Comment seeks to marry the Court's special needs precedent with its border search precedent by analyzing an issue the Court has never ruled on—border searches of electronic property—through a method that is both consistent with existing decisions and grounded in sound logic. Opponents may contend that no shift is necessary at all and that courts should not distinguish digital searches from nondigital ones.[151] But the Court has already noted, without exempting property searches, that any search that occurs in a "particularly offensive manner" may require reasonable suspicion.[152] Therefore, a shift in how courts view digital border searches, which moves away from the extremely deferential treatment of conventional border searches and toward the more scrutinizing special needs test, can be justified if a basis exists for considering these inspections to be significantly more intrusive than searches of nondigital property.

## III. ANALYZING THE IMPACT OF DIGITAL BORDER SEARCHES UNDER THE STATUS QUO

### A. Are Searches of Portable Electronic Devices Meaningfully Different From Searches of Nondigital Containers?

The discussion of the uniqueness of digital border searches has seen many arguments from both extremes of the debate. On one hand, many scholars advocate requiring reasonable suspicion for almost any border search of laptop

149. United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004).

150. *Id.* at 152.

151. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 975–76 (9th Cir. 2013) (en banc) (Callahan, J., dissenting) ("The Supreme Court has been willing to distinguish only between border searches of people and property, not between different types of property. . . . [T]he Court has all but held that property that crosses the border, whatever it is, does not merit Fourth Amendment protection.").

152. *See Flores-Montano*, 541 U.S. at 154–55 n.2 (quoting United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977)).

computers and similar machines.[153] Some argue that travelers have unique privacy expectations in portable electronic devices[154] because of the machines' storage capacities[155] and tendency to contain intimate personal information.[156] By contrast, opponents have reasoned that a container's storage capability has never been a determining factor in the reasonableness of a border search[157] and that searches of nondigital property often reveal private personal information as well.[158]

Ultimately, neither side is wholly correct. Those who eschew any distinction are probably correct in stating that the privacy expectations in a nondigital container can conceivably match those in a laptop computer. Thus, any one search of a portable electronic file is not guaranteed to be more intrusive than any possible search of a conventional container. This Part argues, however, that the increasing ubiquity of people's reliance on mobile electronic devices and the mechanics of computer searches make the average digital border search significantly more intrusive on individuals' Fourth Amendment interests than the average inspection of nondigital property such as a suitcase or a car. Thus, in the aggregate, the proliferation of suspicionless digital border searches could result in a large erosion of American travelers' privacy interests.

### 1. Should Storage Capacity Impact Permissibility?

The storage capacity of mobile devices keeps increasing continually: Current laptop hard drives can hold close to a terabyte,[159] the equivalent of entire li-

153. *See, e.g.*, Joelle Hoffman, Comment, *Reasonable Suspicion Should Be Required at a Minimum for Customs Officials to Execute a Search of a Laptop at U.S. Borders: Why* U.S. v. Arnold *Got It Wrong*, 36 W. ST. U. L. REV. 173, 181 (2009).

154. *E.g.*, Sara M. Smyth, *Searches of Computers and Computer Data at the United States Border: The Need for a New Framework Following* United States v. Arnold, 2009 U. ILL. J.L. TECH. & POL'Y 69, 105 ("[C]ourts must formulate a new legal test that recognizes the uniqueness of these devices and the important privacy interests at stake.").

155. *See, e.g.*, Lindsay E. Harrell, Comment, *Down to the Last JPEG: Addressing the Constitutionality of Suspicionless Border Searches of Computers and One Court's Pioneering Approach in* United States v. Arnold, 37 SW. U. L. REV. 205, 225–27 (2008).

156. 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, 1001 (2007).

157. *See* Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1111 (2009) (noting that even eighteenth century border search statutes drew no distinction between searches of dinghies and searches of 1500-ton ships).

158. Defendants' Memorandum of Law in Support of Motion to Dismiss at 25–26, Abidor v. Napolitano, No. CV 10-4059 (E.D.N.Y. filed Jan. 28, 2011) (noting that routine searches of photographs, medicines, and personal papers would also reveal personal information).

159. To generate this statistic, I researched the hard drive sizes of laptop computers available for sale on BEST BUY, http://www.bestbuy.com (last visited Oct. 28, 2013).

braries' worth of textual information.[160] Thus, a border search of a laptop computer can potentially expose a far greater number of an individual's "belongings" than a search of any physical container. Yet, electronic storage capacity alone should not determine the reasonableness of digital border search. First, the constitutionality of suspicionless border searches of vehicles or physical containers has never depended on their size.[161]

For example, today's largest container ships, which have always been inspected at the border without any suspicion, can carry up to 11,000 twenty-foot-equivalent containers.[162] Though Congress now mandates that every incoming container must be searched using x-rays and radiation scans, courts have never differentiated between containers retrieved from ships of different sizes.[163] Likewise, moving vehicles that hold nearly all the essential possessions of people relocating across the United States' borders are still subject to suspicionless searches.[164] Thus, privileging storage capacity in a Fourth Amendment analysis would conflict with the existing doctrine governing searches of physical containers.

Additionally, the storage capability of an object does not necessarily correlate with the amount of information that the government actually views during the search. For example, an electronic keyword scan, which returns only the few files that contain the terms of interest, discloses far less information to human observation than a manual search of every entry in a person's handwritten address book to identify whether the book contains the contact information of known terrorists.[165] Therefore, the large storage capacity of electronic devices should not itself be a determinative factor in determining the required threshold of suspicion.[166]

160. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005) (stating that an 80 GB hard drive can store the same amount of information as the books in one floor of a typical academic library).

161. United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008) ("Moreover, case law does not support a finding that a search which occurs in an otherwise ordinary manner, is 'particularly offensive' simply due to the storage capacity of the object being searched." (quoting California v. Acevedo, 500 U.S. 565, 576 (1991))).

162. Sales, *supra* note 157, at 1111.

163. *Id.* at 1112.

164. *Id.* (discussing *United States v. Ickes*, 393 F.3d 501, 502 (4th Cir. 2005), in which police thoroughly searched the defendant's van even though it "appeared to contain 'everything he own[ed]'" (alteration in original)).

165. *Id.* at 1120–21.

166. *But see* Harrell, *supra* note 155, at 224–27 (arguing that the storage capacity of computer equipment is one of at least three reasons that border searches of computers are nonroutine).

### 2. Portable Devices' Tendency to Contain Personal Information

Many critics of the current doctrine argue that searches of laptops and other mobile devices are analogous to searches of a person's body, because their owners may use them to store extremely personal, private information.[167] A comprehensive laptop search, for example, can expose intimate data such as a user's personal photos, internet search histories, and email correspondence.[168] Thus, critics reason that searches of laptops, which may expose a person's innermost thoughts, are as intrusive as strip searches or cavity searches that expose the body, which courts subject to a reasonable suspicion standard.[169] This position, however, is difficult to reconcile with longstanding precedent regarding the searches of nondigital items. Courts have already ruled that border searches of items such as personal papers or letters, which may contain similarly expressive, private materials, require no reasonable suspicion. Thus, relying on the personal-search rationale to label border searches of electronic devices as nonroutine would create serious inconsistencies within the border search doctrine that could be remedied only by revisiting decades of precedent.[170]

## B. Unique Risks to Privacy Posed by Searches of Portable Electronic Devices

For the reasons given above, the types of privacy interests infringed by the search of a laptop computer, flash drive, or cell phone are not unique compared to the interests that could possibly be infringed by the search of a nondigital container. This Comment argues, however, that border searches of electronic devices merit additional scrutiny because of the far greater expected loss in privacy (the amount of privacy infringed *on average*) resulting from the search of a laptop computer or other such device at the border.

167. *See, e.g.*, Kindal Wright, Comment, *Border Searches in a Modern World: Are Laptops Merely Closed Containers, or Are They Something More?*, 74 J. AIR L. & COM. 701, 722–23 (2009) (reasoning that laptops are "more accurately analogized to the human body than to a closed container" because they function "as an extension of our own memory" (quoting United States v. Arnold, 454 F. Supp. 2d 999, 1000 (C.D. Cal. 2006)) (internal quotation marks omitted)).

168. Wilson, *supra* note 52, at 1000–01.

169. *Id.* at 1018.

170. *See* United States v. Grayson, 597 F.2d 1225, 1227–29 (9th Cir. 1979) (holding that no suspicion was required for Customs agents to read the content of papers removed from a suspect's breast pocket); *see also* United States v. Seljan, 547 F.3d 993, 1011–12 (9th Cir. 2008) (Callahan, J., concurring) (reasoning that whether the government read the personal correspondence in the defendant's package was irrelevant since suspicionless border searches of property are per se reasonable under the Fourth Amendment).

The first reason why the expected loss resulting from the search of an electronic device will likely be greater is obvious: While it is merely possible that extensive personal information could be exposed in a search of a physical container, this harm is practically guaranteed in any forensic computer search that combs a device's entire memory, such as the kind conducted in *Cotterman* or *Abidor*. Not everyone keeps highly sensitive personal information in their luggage or their vehicle when crossing an international border, but almost everyone has such intimate material in their laptop, iPhone, or other digital device—whether saved in folders, in their browser, email, or chat history, or in the unallocated space that holds files that they deleted in the past.[171] The Constitution Project, a civil libertarian think tank, advanced this argument in a 2011 report:

> Historically, the scope of what was covered by the border search exception was fairly limited, since the exception is confined to the items a traveler carries across the border. As a practical matter, most private documents, letters, photographs, and other personal effects would remain in an individual's home, safeguarded by full Fourth Amendment protections and the warrant requirement. With today's technology, however, people can and do travel with vast quantities of private, personal information stored on their laptops and other electronic devices. Unlike at any time in the past, individuals who travel internationally, by virtue of legitimately choosing to carry electronic devices, are unknowingly subjecting volumes of personal information to involuntary and suspicionless search and review by federal law enforcement authorities. This problem is compounded by the fact that many electronic devices are used to carry both personal and business-related information. The continual evolution in how people use electronic devices in their everyday lives creates growing tension between the Fourth Amendment guarantees and what historically has been viewed as a narrow exception to the requirements for probable cause and a warrant.[172]

171. *See* Mark Rasch, *On the Border*, SECURITY FOCUS (Mar. 20, 2008), http://www.securityfocus.com/columnists/469/2 ("While most people do not travel internationally with a copy of every chat they have ever had, or every Facebook friend's picture in their Samsonite, or every picture they have of their boyfriends or girlfriends, they have exactly this information on their laptops. They have their checkbook information, passwords, financial records, medical records, correspondence, records of books purchased, Web sites reviewed, and more.").

172. THE CONSTITUTION PROJECT, SUSPICIONLESS BORDER SEARCHES OF ELECTRONIC DEVICES: LEGAL AND PRIVACY CONCERNS WITH THE DEPARTMENT OF HOMELAND SECURITY'S POLICY 2 (2011).

A potential counterargument might be that travelers store such information in their portable devices only because they are not aware that laptops and cell phones are subjected to border searches.[173] Thus, as more people become aware of the current CBP and ICE polices, they might stop storing such sensitive information on mobile devices or avoid bringing these devices when traveling internationally. These types of changes in practice, however, would likely be prohibitively inconvenient for many travelers, especially those in the business world. For example, in the wake of *Arnold*, some business executives indicated that avoiding international travel altogether would be more cost effective than taking new measures to ensure that border searches of their laptops did not reveal sensitive information.[174] Consequently, since there is no indication that Americans will rely any less on mobile devices, regardless of current CBP and ICE policies, we should be especially concerned about the likelihood that searches of these devices will reveal personal information.

The massive quantity of personal information that can be potentially observed in any border search is harmful not just because of the information's value to the traveler. The government's ability to access a large amount of personal data also gives agents a greater incentive to abuse the border search doctrine by turning searches into "potential[ly] unfettered dragnet[s]" that serve only general law enforcement purposes.[175] For example, in *House*, agents never indicated what crime they meant to investigate by detaining the suspect's computer.[176] Consequently, one might hypothesize that the government had no particular interest in border security but was instead conducting a "fishing expedition" against House as a means of harassment or retaliation because of his political activities.[177] Because such suspicionless searches are not illegal in the majority of jurisdictions that are not beholden to the *Cotterman* ruling, the government could easily use its digital border search powers as a pretext to investigate a suspect for crimes that have no significance to the border. Since nearly any piece of

173. *Cf.* David Jonas, *Airport Laptop Seizures Debated in Washington*, BUS. TRAVEL NEWS (July 9, 2008, 6:56 PM), http://www.businesstravelnews.com/Business-Travel/Airport-Laptop-Seizures-Debated-in-Washington (discussing a survey that revealed that 62 percent of travel industry executives polled were unaware that electronic devices could be seized at the border without a warrant).

174. *Id.*

175. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) (en banc).

176. *See* House v. Napolitano, No. 11-10852-DJC, 2012 WL 1038816, at *4 (D. Mass. Mar. 28, 2012).

177. *Cf.* Matthew Lasar, *Critics Demand Halt to "Fishing Expedition" Laptop Searches*, ARS TECHNICA (May 20, 2011, 7:14 AM), http://arstechnica.com/tech-policy/2011/05/critics-demand-halt-to-fishing-expedition-laptop-searches (noting House's statement that the DHS's questioning primarily revolved around his political beliefs and his connection to the Bradley Manning Support Network).

data on a suspect's computer can potentially contain evidence of a crime that is relevant to border security, CBP, without suspicion, could trawl a suspect's entire computer under the guise of searching for violations of laws they are tasked with enforcing.[178] After finding evidence of an unrelated crime, such as perjury, the government could then use the Fourth Amendment's plain view doctrine to prosecute the suspect for this latter offense.[179] By contrast, because a vehicle, suitcase, or other type of physical container is highly likely to hold a far smaller amount and variety of information than a computer, the government would have less incentive to engage in such an arbitrary and thorough search, since agents would be much less likely to find any incriminating material.[180] Although the Supreme Court has never held that border agents can inspect traveler's property only for evidence of crimes that are especially pernicious,[181] general Fourth Amendment jurisprudence makes clear that searches exempted from warrant and probable cause requirements are not meant to serve ordinary law enforcement goals.[182] Thus, courts should be especially wary of any doctrine that could provide the government with a loophole for pursuing such fishing expeditions.

A second important distinction between searches of digital devices and searches of physical containers is that forensic-search software allows an agent to probe parts of the device that most users do not know how to access. For example, the inspecting analyst can search unallocated or slack disk space—the part of the hard drive containing files that the user previously deleted.[183] By default, the machine's operating system does not physically erase the file—it only marks the previously occupied space as free for reuse, allowing its contents to be

178. *See infra* note 206 and accompanying text.

179. The plain view doctrine holds that when the government is executing a permissible search and, without expanding the scope of the search beyond its permissible bounds, encounters potentially incriminating evidence, the government can seize the evidence and use it for prosecution even if the evidence was not the target of the original search. *See* 3 LAFAVE, *supra* note 144, § 6.7. For a case applying the plain view doctrine in a border search context, see *United States v. Seljan*, 547 F.3d 993 (9th Cir. 2008), in which customs inspectors searched the defendant's FedEx packages for undeclared currency or monetary instruments and subsequently encountered "immediately apparent" evidence of pornography and pedophilia. *Id.* at 996–97, 1006. The government used the material as evidence against the defendant and subsequently charged him with multiple sex crimes. *Id.* at 996. When the defendant moved to suppress all evidence found during the search of his FedEx packages, the district court denied the motion and the appellate court, citing the plain view doctrine, upheld the district court's decision. *Id.* at 1005–06.

180. *Cf. Cotterman*, 709 F.3d at 964 ("The private information individuals store on digital devices . . . stands in stark contrast to the generic and impersonal contents of a gas tank.").

181. *See supra* Part II.C.

182. *See supra* Part II.C.

183. Kerr, *supra* note 160, at 542.

recovered as long as a new file does not begin occupying that space.[184] Freeware utilities that physically overwrite a file's previously used space with random information can be downloaded from the internet,[185] but most users are not aware of such utilities, or even of the mechanism that recycles purportedly deleted file space.[186] By contrast, nearly all individuals are aware of their ability to remove personal items from their luggage or vehicles before their travels if they do not want to expose the property to authorities in the event of a search.[187] Thus, a laptop computer search has a greater likelihood of violating a serious privacy interest than does a physical container search.

Moreover, as the Ninth Circuit recently noted in *Cotterman*, digital border searches, unlike conventional border searches, may result in the government accessing information that did not actually cross the border.[188] Many travelers use cloud computing technology to store personal information through remote servers, such as DropBox or Google Drive, which allow them to access the information through the internet without storing the data on their machines.[189] If government agents search a computer in which the individual has automatically saved his passwords to these accounts, they could then check for digital contraband on these servers. In this type of search, the government could potentially use a piece of property that a traveler transported across the international border (for example, a laptop or iPhone) as a means to prosecute the individual for possessing property that never moved (for example, a pirated file inside an online drop box).[190] This search would be legally problematic because the border search doctrine would provide the legal basis for an inspection to which the doctrine's justification could not apply; the need to prevent the entry or exit of contraband is not served by searching files that the suspect never transported to the border.

184. *Id.*

185. One such available program that overwrites unallocated space to prevent the recovery of files the user deletes is WipeFile. *See WipeFile*, GAIJIN, http://www.gaijin.at/en/dlwipefile.php (last visited Oct. 28, 2013).

186. *See Cotterman*, 709 F.3d at 965 ("Electronic devices often retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files. This quality makes it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel.").

187. Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss at 23, Abidor v. Napolitano, No. CV 10-4059 (E.D.N.Y. filed Mar. 9, 2011) ("[I]t is nearly impossible to effectively remove private information from electronic devices in the same way that one could leave a sensitive file at home or take it out of a briefcase prior to crossing the border.").

188. *See Cotterman*, 709 F.3d at 965.

189. *Id.*

190. *See id.*

In addition to the mechanics of digital file storage, the potential for an electronic device to be detained indefinitely by the government and searched for an extended period of time provides another reason to suspect that such searches are more intrusive than searches of physical containers.[191] Because computers can store so much information, a comprehensive forensic search that probes the entire device's memory, should a logical or keyword search for certain terms not reveal any evidence of criminal activity, may take weeks to complete.[192] For example, DHS has admitted that searches can, on rare occasions, last up to six months.[193] Moreover, the potential need to search a laptop computer for more than a few hours is not the only reason the government might detain property for a prolonged period. Sometimes, the port of entry or border station may lack the software needed to decrypt computer passwords or conduct comprehensive searches, making it necessary to transfer the property to a site with the requisite forensic software.[194] By comparison, searches of typical physical containers that travelers ordinarily transport internationally, like suitcases or vehicles, can usually be completed much more quickly.[195] For example, in *Flores-Montano*, border agents were able to summon a mechanic to take apart the gas tank of the defendant's car and remove thirty-seven kilograms of marijuana within an hour.[196] Thus, because computer searches are more likely than physical container searches to deprive travelers of their possessory interest in their property for an extended period of time, such inspections, on average, pose greater harm to an individual's Fourth Amendment interests.[197] Therefore, because a digital border search is highly likely to be more intrusive than a conventional inspection, a basis exists for subjecting the former to a more exacting Fourth Amendment standard.

191. *See* United States v. Place, 462 U.S. 696, 710 (1983) (holding that the prolonged detention of the suspect's luggage and removal of his bags to an undisclosed location contributed to a finding that the seizure was unreasonable under the Fourth Amendment).
192. Kerr, *supra* note 160, at 544.
193. *See* THE CONSTITUTION PROJECT, *supra* note 172, at 5 (discussing DHS documents made public through a Freedom of Information Act lawsuit which revealed "one instance" in which "a traveler had a laptop computer and flash drive confiscated by CBP, and over six months later, he was still trying—with the help of his congressman—to secure the return of his possessions").
194. *See supra* Part III.A (describing the facts of *Cotterman*).
195. *See* Kerr, *supra* note 160, at 543–44.
196. United States v. Flores-Montano, 541 U.S. 149, 150–51 (2004).
197. Note, however, that the government detains electronic devices for an extended period of time only in less than 5 percent of inspections. *See* THE CONSTITUTION PROJECT, *supra* note 172, at 4 (noting that in the first eight months of fiscal year 2009, CBP conducted 2204 searches of electronic devices and made 105 detentions).

### C. How Is Current Government Policy on Laptop Border Searches Impacting These Privacy Concerns?

In August 2009, CBP and ICE released directives (hereinafter, the Directives) that established policies for their agents to follow when conducting border searches of electronic devices.[198] The Directives contain safeguards to prevent misuse of or tampering with property,[199] disclosure of privileged information,[200] and indefinite retention and search of copies of materials,[201] and to require transparency about the purpose and scope of searches.[202] Unfortunately, the policies also fail to protect individuals' Fourth Amendment interests in several ways. First, both documents explicitly state that agents did not need individualized suspicion to conduct a border search.[203] In fact, in January 2013, the DHS's Office for Civil Rights and Civil Liberties reaffirmed the government's position that "CBP's and ICE's current border search policies comply with the Fourth Amendment" and "that imposing a requirement that officers have reasonable suspicion in order to conduct a border search of an electronic device would be operationally harmful without concomitant civil rights/civil liberties benefits."[204] Moreover, despite requirements that any border search remain consistent with its original purpose and scope, the Directives make clear that the number of laws at the border that the two agencies enforce is so long and diverse that a search of almost any scope could seemingly be justified:

> As the Nation's law enforcement agencies at the border, CBP interdicts and ICE investigates a range of illegal activities such as child

198. *See* U.S. CUSTOMS & BORDER PROT., CBP DIRECTIVE NO. 3340-049, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION (2009) [hereinafter CBP DIRECTIVE]; U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, ICE DIRECTIVE NO. 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES (2009) [hereinafter ICE DIRECTIVE]. The directive defined electronic devices as "any devices that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices." CBP DIRECTIVE, *supra*, at 2.

199. ICE DIRECTIVE, *supra* note 198, at 4 (describing the requirements for maintaining a proper chain of custody).

200. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE BORDER SEARCHES OF ELECTRONIC DEVICES 13 (2009) [hereinafter PIA] ("ICE policy and certain laws, such as the Privacy Act and the Trade Secrets Act, requires the special handling of some types of sensitive information including attorney-client privileged information, proprietary business information, and medical information.").

201. CBP DIRECTIVE, *supra* note 198, at 4; ICE DIRECTIVE, *supra* note 198, at 8.

202. PIA, *supra* note 200, at 17–20.

203. CBP DIRECTIVE, *supra* note 198, at 3; ICE DIRECTIVE, *supra* note 198, at 2.

204. TAMARA KESSLER, U.S. DEP'T OF HOMELAND SEC. OFFICE FOR CIVIL RIGHTS & CIVIL LIBERTIES, CIVIL RIGHTS/CIVIL LIBERTIES IMPACT ASSESSMENT: BORDER SEARCHES OF ELECTRONIC DEVICES 1 (2012).

> pornography; human rights violations; smuggling of drugs, weapons, and other contraband; financial and trade-related crimes; violations of intellectual property rights and law (e.g., economic espionage); and violations of immigration law, among many others. CBP and ICE also enforce criminal laws relating to national security, terrorism, and critical infrastructure industries that are vulnerable to sabotage, attack or exploitation.[205]

As discussed above, border agents enforce a highly disparate set of laws, and evidence of the laws' violation could conceivably be found in all types of electronic information. For example, a person's email correspondence could contain evidence of a terrorist conspiracy; his video, picture, and software files could contain pirated material; and his search history could reveal attempts to procure child pornography. Thus, a border agent could likely argue that the authority to enforce these laws justifies a comprehensive forensic search of any laptop.[206]

The Directives not only support border agents' authority to enforce a wide range of laws but also set no limits on when agents can conduct exhaustive, forensic computer searches or detain property for closer inspection. In fact, the DHS's Privacy Impact Assessment, though not requiring that agents meet any evidentiary burden before detaining a device, implied that a detention was reasonable nearly any time that an on-site search would pose an inconvenience:

> Many factors may result in a detention, for example, time constraints due to connecting flights, the large volume of information to be examined, the need to use off-site tools and expertise during the search (e.g., an ICE forensic lab), or the need for translation or other specialized services to understand the information on the device.[207]

Lastly, the ICE Directive gives the agency a troublingly free reign over detentions, even surpassing the broad authority of CBP. While the CBP Directive states that "[u]nless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days,"[208] its ICE counterpart merely states that "Special Agents are to complete the search of detained electronic devices . . . in a reasonable time," and specifies that "[s]earches are generally to be

205. PIA, *supra* note 200, at 4.

206. *See* Kelly A. Gilmore, Note, *Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border*, 72 BROOK. L. REV. 759, 761 & n.13 (2007) (stating that the CBP enforces "over 400 laws on behalf of over forty federal agencies" and reasoning that information on mobile electronic devices is needed for the successful prosecution of many of these offenses).

207. PIA, *supra* note 200, at 5.

208. CBP DIRECTIVE, *supra* note 198, at 4.

completed within 30 calendar days of the date of detention."[209] Furthermore, while CBP detentions of more than fifteen days can be extended only seven days at a time,[210] extensions of ICE detentions beyond thirty days can occur in fifteen-day increments.[211] Thus, despite the Directives' limitation on how digital information can be handled and retained, the policy nonetheless fails to address many of the serious privacy concerns that are likely to be at issue in digital border searches.

### D. Past Legislative Proposals to Regulate Border Searches of Electronic Devices

The failures of recent Congressional efforts to curb digital border searches demonstrate how unlikely it is that the United States will implement legislation requiring individualized suspicion for inspections of portable electronic devices. In 2009, for example, two legislators introduced bills that would have imposed additional requirements for border searches of laptops, neither of which passed.[212] The Securing Our Borders and Our Data Act of 2009,[213] introduced by Representative Eliot Engel (D-NY), would have allowed searches of portable electronic devices only on at least reasonable suspicion, and the bill would have allowed seizures of the property only if justified by constitutional authority other than the traditional border search authority. Moreover, the bill would have directed the Secretary of Homeland Security to promulgate rules establishing maximum time periods for detentions of property seized in border searches, owners' rights to reclaim detained devices, and protections for the sanctity of any information detained and shared with other federal agencies.[214]

A second bill, the Border Security Search Accountability Act of 2009,[215] introduced by Representative Loretta Sanchez (D-CA), did not impose a reasonable suspicion threshold for digital border searches, but it would have required the Commissioner of CBP to promulgate a rule requiring that (1) "commercial information be handled in a manner consistent with all laws and regulations governing such information;" (2) "electronic searches be conducted

209. ICE DIRECTIVE, *supra* note 198, at 4–5.
210. CBP DIRECTIVE, *supra* note 198, at 4.
211. ICE DIRECTIVE, *supra* note 198, at 5.
212. Sunil Bector, Note, *"Your Laptop, Please:" The Search and Seizure of Electronic Devices at the United States Border*, 24 BERKELEY TECH. L.J. 695, 712–13 (2009).
213. H.R. 239, 111th Cong.
214. YULE KIM, CONG. RESEARCH SERV., RL34404, BORDER SEARCHES OF LAPTOP COMPUTERS AND OTHER ELECTRONIC STORAGE DEVICES 13–14 (2009).
215. H.R. 1726, 111th Cong.

in front of a supervisor;" (3) "the number of days commercial information could be retained without probable cause be determined;" (4) "the individual whose information was seized be notified if the information is entered into an electronic database;" (5) "an individual receive a receipt if his device is seized during a border search;" and (6) "an individual subject to a border search of an electronic device receive notice as to how he can report any abuses or concerns."[216] Though Congress never passed Sanchez's bill, the Directives incorporated five out of the six proposed requirements (all but the second requirement).[217] Thus, while legislative efforts may successfully induce the government to promote transparency in border search procedures, they have failed to prevent CBP and ICE from conducting digital searches without reasonable suspicion.

## IV. WHEN SHOULD REASONABLE SUSPICION BE REQUIRED FOR A DIGITAL BORDER SEARCH?

Because the executive and legislative branches have proved unwilling and unable to subject any type of digital border search to a reasonable suspicion standard, reform is most likely to come from the judiciary. Moreover, the previous Part's conclusions demonstrate that digital border searches are meaningfully different from conventional border searches because they are more likely to infringe a suspect's Fourth Amendment interests.[218] Thus, courts should take the lead in subjecting these inspections to a greater degree of constitutional scrutiny.[219]

Although some scholars have advocated subjecting all border searches of electronic devices to a reasonable suspicion standard,[220] such a drastic doctrinal shift would be illogical, since certain digital searches can be much less intrusive than many searches of nondigital containers, which do not require any suspicion.[221] Consequently, a better method is to submit any digital border search to a balancing test that weighs the government's law enforcement interest against the harm to an individual's Fourth Amendment interests. A search in which

216. KIM, *supra* note 148, at 20.
217. *See* PIA, *supra* note 200, at 5, 7–9, 12–13, app. A.
218. *See supra* Part III.B.
219. *See supra* Part III.B.
220. *See, e.g.*, Smyth, *supra* note 154, at 105 ("At a minimum, the search of electronic storage devices should be characterized as nonroutine . . . and thus must be preceded by reasonable suspicion.").
221. *See supra* note 165 and accompanying text (describing the minimal relative intrusiveness of electronic keyword searches as compared to searching a physical address book); *supra* note 170 and accompanying text (discussing court holdings that border searches of certain physical items require no reasonable suspicion even when they reveal highly private information, such as personal correspondence).

the balance favored the government would likely be permitted without particularized suspicion, and a search in which the balance favored the individual would likely require at least reasonable suspicion.

### A. Special Needs–Style Balancing Test

Since border searches are so analytically similar to special needs searches,[222] a proper balancing test for digital border searches should draw inspiration from the special needs test. In a traditional special needs analysis, a court first determines the government's law enforcement interest by asking whether the search serves a special governmental need, distinct from the needs of ordinary law enforcement, which would be difficult to fulfill if a warrant and probable cause were required for the search.[223] If no such need exists, there can be no relaxation of Fourth Amendment protections.[224] If the search indeed serves a special need, however, the court must also calculate the government's interest by considering the magnitude[225] of the problem that the government is addressing and the effectiveness[226] that the disputed search or seizure, at the lower-than-ordinary level of suspicion, would have in combating such a problem. Then, the court must determine whether the government's interest outweighs the individual interests that the search infringes.[227] If the court concludes that the government's interest is stronger, the search is constitutionally permissible.[228]

This Comment's proposed balancing test differs from the traditional special needs test in two ways. First, because of the Supreme Court's historic deference toward conventional property searches at the border, a model for evaluating digital border searches should be tailored to avoid outcomes that are logically inconsistent with existing border search precedent regarding traditional searches.[229] In particular, the determination that the disputed search serves a

222. *See supra* note 52 and accompanying text.
223. *See supra* Part I.B.
224. *See supra* Part I.B.
225. *See* Chandler v. Miller, 520 U.S. 305, 318 (1997) (reasoning that Georgia's suspicionless drug testing of political candidates was not justified because "the proffered special need . . . must be substantial . . . to suppress the Fourth Amendment's normal requirement of individualized suspicion").
226. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 660–64 (1995) (considering "the efficacy of [the] means for addressing the problem" in deciding whether a public school's suspicionless drug testing of student athletes was justified as a special needs search).
227. *See supra* Part I.B.
228. *See supra* Part I.B.
229. *See* Erick Lucadamo, Note, *Reading Your Mind at the Border: Searching Memorialized Thoughts and Memories on Your Laptop and* United States v. Arnold, 54 VILL. L. REV. 541, 574 (2009) (discussing

special need should not be an absolute prerequisite to finding the search reasonable. This modification is necessary to prevent situations in which the government would not be legally permitted to conduct any digital search for certain information without suspicion yet would be permitted to conduct a suspicionless search for the same information through more intrusive conventional means. Such scenarios would arise because courts may conclude that some of the laws enforced by the CBP do not fulfill a special governmental need at the border.[230] Under a conventional special needs analysis, if a court made this determination, ordinary Fourth Amendment requirements of individualized suspicion would apply regardless of the search's intrusiveness.[231] Yet, had the same crime been investigated through a border search of a nonelectronic physical container, existing border search precedent dictates that such a search would be permissible without any particularized suspicion.[232] Therefore, to avoid this inconsistency, the special need question should not be determinative.[233] Rather, the court should conclude that the government still has a valid, albeit lower, interest in effectively enforcing the law in question through a suspicionless digital border search.

Second, for the sake of predictability, a court should not adjust the government's interest depending on the magnitude of the problem addressed by the enforced statute and the search's effectiveness in combating the problem. Given that CBP and ICE enforce over 400 laws, many of them completely unrelated to one another,[234] a court's determination of the interest and effectiveness of an inspection in enforcing any one of these laws would be highly subjective. Thus, the conventional balancing test would have little predictive value for the constitutionality of the government's enforcement of a different law at the border, leaving both border agents and travelers with little idea of when particularized suspicion is required. Therefore, courts should simplify the test when applied to

"the impracticalities that would occur if laptops were given a novel and unique status unlike other objects crossing the international border").

230. *See infra* Part IV.A.1, discussing the CBP's enforcement of racketeering laws that have no unique significance at the border.

231. *See, e.g.*, City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (holding that when a search serves no special need but only a general interest in criminal investigation, there is a "usual requirement of individualized suspicion").

232. *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 . . . even without any specific suspicion concerning its contents.").

233. *See* Sales, *supra* note 157, at 1128 (stating that "[p]rivacy rights should not be determined by mere fortuities" such as "the medium in which [the traveler] keeps [information]").

234. *See, e.g.*, U.S. CUSTOMS & BORDER PROT., SUMMARY OF LAWS AND REGULATIONS ENFORCED BY CBP (2008) [hereinafter SUMMARY OF LAWS].

digital border searches. While courts should assign the government's interest a higher weight in any inspection that fulfills a special need at the border and a lower weight if no such need can be shown, these weights should not vary depending on the law enforced and the search method used. In conclusion, this model condenses the standard two-part special needs test into a single balancing test that weighs the government's interest, which varies solely based on whether there is a special need for the search, against the totality of the harms to an individual's Fourth Amendment interests.

#### 1. The Government's Interest—Does the Search Serve a Special Need?

Courts can most easily answer the special need question by asking whether the search is seeking evidence of a crime that, because of its statutory definition, can be committed or has particular significance only when committed during a border crossing. The government has a special need in preventing such crimes at the border because, once the suspect has cleared the checkpoint, the commission of the offense (for example, the transmission of prohibited material across the border or the failure to present certain information at the border) will have reached completion.[235] Thus, when the potential legal violation being investigated meets this criterion, the likelihood of the search's permissibility should increase.

Most of the laws that CBP and ICE enforce will likely fall into this category. For example, many of the laws enforced at the border are prohibitions on transporting unauthorized immigrants or items such as banned agricultural products, drugs, illegal digital files, weapons, and child pornography across the border.[236] Border agents also enforce many laws that mandate the disclosure of certain information at the border, such as whether the traveler is carrying legal documents, dutiable goods, or large amounts of currency.[237] Furthermore, CBP and ICE also enforce statutes prohibiting certain behavior during a border crossing, such as attempting to bribe an officer[238] or destroying property at the border to prevent its seizure.[239] Ordinary law enforcement officials, who do not police the border, cannot prevent these laws from being broken; the prohibited

235. *See generally id.* for a list of the laws enforced by CBP agents.
236. *See generally id.*
237. *See id.* at 3 (noting enforcement of 8 U.S.C. § 1181 (2012)); *id.* at 15 (noting enforcement of 19 U.S.C. §§ 1202–1677 (2012)); *id.* at 21 (noting enforcement of 31 U.S.C. §§ 5301–5326 (2012)).
238. *See id.* at 9–10 (noting enforcement of 18 U.S.C. §§ 205–225 (2012)).
239. *See id.* at 13 (noting enforcement of 18 U.S.C. § 2232 (2012)).

act will already have been completed once the person or property fully crosses the border. Thus, there is a special need for CBP and ICE to investigate for violations of these laws. Since border agents have limited information about the background of each traveler, and since travelers can often conceal evidence of such crimes from plain view, requiring individualized suspicion for every border inspection would destroy the government's ability to prevent such infractions.

The CBP and ICE are also, however, responsible for enforcing laws that do not have particular significance at the border. For example, the agencies enforce 18 U.S.C. §§ 1951, 1961–1968 (2012), which are antiracketeering laws.[240] These laws make no reference to whether the prohibited actions occur domestically, overseas, or transnationally.[241] Hence, it would be much harder for the government to make the case that there was a special need to search a suspect at the border in order to enforce these laws. Therefore, a suspicionless computer border search to detect a crime such as racketeering should be less permissible than a search for a crime such as the importation of child pornography, whose transportation into the United States is specifically prohibited by statute.[242]

**a. Digital Versus Physical Contraband**

Many critics of the status quo argue that that the government does not have a special need to search for digital contraband at the border.[243] First, they contend that when the border search doctrine originated, it was intended to combat only the smuggling of physical contraband, such as drugs and dutiable goods.[244] Second, these critics reason that digital border searches cannot fulfill a special need because they would not be effective in keeping the information out of the country; a criminal outside the United States could simply transfer the material to a user within the country through email or an online drop box.[245] Neither of these arguments, however, makes a persuasive case for subjecting any and every search for digital contraband to a higher evidentiary standard.

The first argument is unconvincing because, even though electronic files did not exist when the border search exception originated, digital contraband,

240. *See id.*
241. *See* 18 U.S.C. §§ 1951, 1961–1968 (2012).
242. *See id.* § 2252.
243. *See, e.g.*, Wilson, *supra* note 52, at 1025.
244. *See* Marianne Leach, *Flyers Beware: The Ninth Circuit Decision*, United States v. Arnold, *Granted Customs Agents Access Into Your Laptops*, 26 T.M. COOLEY L. REV. 307, 345 (2009) (arguing that "many of the strong government[al] interests do not apply to digital information" because "[t]he border-search exception was created to deal with issues that came about before the digital world—to protect the country from physical intrusions and dangers").
245. *See* Wilson, *supra* note 52, at 1017.

just like drugs or banned agricultural products, cannot be legally imported or exported. Identifying the traffic of prohibited materials at the border has always been a purpose of the border search exception. Therefore, the government clearly has a special need to locate digital contraband. Moreover, the United States' history of seizing the types of contraband that now tend to be digitized greatly predates the advent of personal electronic devices. For example, many of the government's electronic border searches today are intended to detect the transportation of illegal pornography into the country. Yet, well before the advent of laptop computers, customs agents were already searching containers at the border for pornography stored in nondigital media such as film and printed photographs.[246] Thus, while personal electronic devices may be relatively new, the special need for identifying the type of material stored on digital media has existed for far longer. Although courts currently give too much weight to the government's interest in conducting a digital border search relative to the individual's interest, categorically restricting the doctrine to nondigital storage media would create the opposite problem. Instead, courts should adopt a model that reconciles new means of storage and investigation with traditional state interests at the border.[247]

As with the first argument, the second argument—that trying to keep out digital information through border searches is futile—does not sufficiently distinguish digital property from conventional containers. In fact, the government is neither as successful at keeping out physical contraband nor as unsuccessful at keeping out digital contraband as critics imply. For example, empirical evidence demonstrates that the United States has failed to prevent drugs[248] or unauthorized immigrants[249] from entering the country, but courts still allows the CBP

246. *See* United States v. 12 200-ft. Reels of Super 8MM. Film, 413 U.S. 123 (1973).

247. In fact, the Supreme Court has already demonstrated in other contexts how Fourth Amendment jurisprudence can be updated to accommodate the existence of new technologies while preserving traditional privacy expectations. For example, thermal imaging devices did not exist when the Fourth Amendment was written. Nevertheless, the Court has held that the use of such technology to measure heat inside a home constitutes a search under the Fourth Amendment because of its capture of private information from the interior of one's residence. *See* Kyllo v. United States, 533 U.S. 27, 34–45 (2001).

248. Eduardo Porter, *Numbers Tell of Failure in Drug War*, N.Y. TIMES, July 3, 2012, http://www.nytimes.com/2012/07/04/business/in-rethinking-the-war-on-drugs-start-with-the-numbers.html (noting that, despite the efforts of American and Mexican law enforcement, the price of cocaine has dramatically dropped in the last thirty years, which suggests that the supply is increasing).

249. Julia Preston, *11.2 Million Illegal Immigrants in U.S. in 2010, Report Says; No Change From '09*, N.Y. TIMES, Feb. 2, 2011, at A15 (noting that a "Pew report suggests that the high numbers of unauthorized immigrants are confounding enforcement efforts by the Obama administration and also a recent spate of measures by state legislatures to crack down locally on illegal immigration").

and ICE to search people's vehicles for both without any particularized suspicion. Therefore, requiring the government to be wholly successful in preventing digital contraband from crossing our borders would be inconsistent with the legal precedent applied to suspicionless searches for nondigital contraband.

Moreover, just as border searches occasionally do succeed in stopping the trafficking of physical contraband, border searches do sometimes prevent the trafficking of digital contraband. First, forensic searches can retrieve files that the user deleted but did not fully wipe from the device's memory. Therefore, someone who emails an illegal file to himself or others from abroad, deletes it from the recycle bin on his laptop, and then crosses the border with the computer, may nonetheless be apprehended and prevented from committing similar crimes in the future.[250] Second, the government's ability to conduct such searches may deter those who travel internationally from acquiring digital contraband in the first place because of concern that they will be caught with it and arrested when they cross the border with the electronic storage device. Thus, the government's efforts to confiscate digital contraband are capable of similar successes and failures to its efforts to stop physical contraband. Consequently, the former deserves a special needs designation.

### 2. Calculating the Fourth Amendment Interests Infringed by Electronic Border Searches

This Comment proposes that the privacy interests of the individual in any nondestructive electronic border search be calculated according to the totality of three considerations that the Supreme Court, in both border search cases and other special needs cases, has considered relevant to an individual's Fourth Amendment rights.

First, a court should examine the amount and nature of the information inspected by the government in the search. As the Supreme Court has previously indicated, a search that gathers more information is more intrusive.[251]

250. For example, in *Cotterman*, agents found all the files containing child pornography in the defendant's unallocated space. *See* United States v. Cotterman, 637 F.3d 1068, 1072 n.5 (9th Cir. 2011) (defining unallocated space).

251. *See* United States v. Martinez-Fuerte, 428 U.S. 543, 557–58, 566–67 (1976) (upholding suspicionless stops of individuals at permanent checkpoints near the border to inspect for unauthorized immigrants when "the consequent intrusion on Fourth Amendment interests [was] quite limited," since the suspects were only asked a few brief questions and were asked to provide only one document evidencing the right to be in the United States); United States v. Brignoni-Ponce, 422 U.S. 873, 880 (1975) (noting "the limited nature of the intrusion" in part because the border patrol did not inspect the vehicle or its occupants). Sometimes, the information gathered by the government is so minimal that the Court has ruled that the inspection does not even constitute a

Similarly, an individual's privacy interests will be harmed to a greater degree if the search reaches content in which he or she has a large expectation of privacy.[252] In the special needs and conventional border search contexts, courts have applied this principle by upholding suspicionless searches, such as DUI[253] or unauthorized immigration checkpoints,[254] which uncover only small amounts of relatively nonintimate information. But special needs searches that gather a greater quantity of highly personal information, such as strip searches, have sometimes been found unconstitutional even when performed based on reasonable suspicion.[255] Hence, the permissibility of suspicionless electronic border searches should depend in part on the nature and amount of the information collected.

For electronic searches, the depth of the search would likely affect a court's assessment of this factor. For example, a forensic search, such as the one in *Cotterman*, would be more intrusive than a nonforensic search, such as the one in *Arnold*, which would not probe as deeply into the computer's storage.[256] The forensic software that agents use to trawl a computer's memory is often capable of recovering deleted files, logs showing the step-by-step details of a person's computer and internet usage, and transcripts of emails and chats. Such software can also often crack weak passwords that guard personal data.[257] On the other hand, a nonforensic search, in which the agent used no special investigatory software to view the device, would generally give the government access to significantly less information.[258] Similarly, once government agents have accessed a device's memory, the means by which they probe and flag suspicious infor-

Fourth Amendment search. For example, in *United States v. Place*, the court ruled that a dog sniff of a traveler's luggage, which revealed nothing more than the presence or absence of narcotics, "did not constitute a 'search' within the meaning of the Fourth Amendment," because the "investigative procedure [was] so limited both in the manner in which the information [was] obtained and in the content of the information revealed by the procedure." 462 U.S. 696, 707 (1983).

252. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447, 451–52 (1990) (characterizing "the measure of the intrusion" on the individual as "minimal" because of the limited inspection of motorists at a highway checkpoint for signs of intoxication); *Brignoni-Ponce*, 422 U.S. at 880 (noting "the limited nature of the intrusion" in part because the Border Patrol's visual inspection of the suspect's car was "limited to those parts of the vehicle that . . . [could] be seen by anyone standing alongside").

253. *See Sitz*, 496 U.S. at 451–52.

254. *See Martinez-Fuerte*, 428 U.S. at 566–67.

255. *See* Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 374–77 (2009).

256. See *supra* Part II.B for a description of the searches used in these cases.

257. ORG. OF AM. STATES, COMPUTER FORENSIC CAPABILITIES 3 (2010), http://www.oas.org/juridico/english/cyb_mex_forensic_out.pdf.

258. United States v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013) (en banc) ("It is the comprehensive and intrusive nature of a forensic examination . . . that is the key factor triggering the requirement of reasonable suspicion here.").

mation would also be relevant to this factor. For instance, a keyword search of the individual's files, which exposes only the files containing the searched for terms to human observation, would be more respectful of an individual's privacy interests than a search in which the agent viewed the content of a large number of files, including those that store no incriminating information, in order to find contraband.[259] Therefore, searches that are nonforensic and that reveal minimal information to human observation would be more likely to be permissible without any level of suspicion.

Second, courts should consider the duration of the search in evaluating the harm to the individual's constitutional rights. The Supreme Court has established in border search cases[260] and other special needs cases[261] that "the brevity of the invasion of the individual's Fourth Amendment interests is an important factor" in determining the intrusiveness of the search.[262] This factor's relevance stems from the Fourth Amendment's protection against unreasonable seizures, since a government detention of a person[263] or his or her property[264] for the purpose of a search is a seizure. Moreover, this factor cuts against the government even if agents copy the suspect's hard drive, return the original device promptly, and search the copy. Searching a copy still interferes with the suspect's privacy interest in the information itself, so the Fourth Amendment seizure will not

259. *See* Sales, *supra* note 157, at 1123 (comparing keyword searches to searches in which the agent manually peruses the contents of the hard drive).

260. *See* United States v. Martinez-Fuerte, 428 U.S. 543, 546–47, 557–58 (1976) (noting that the Fourth Amendment intrusion was "quite limited" in stops of motorists at checkpoints near the border that lasted only "three to five minutes"). Additionally, though the holdings in these cases arguably depended on the entity searched rather than the length of the search, compare *United States v. Flores-Montano*, 541 U.S. 149, 151 (2004), which held that no suspicion was required for a detention of less than an hour to search a suspect's gas tank, with *United States v. Montoya de Hernandez*, 473 U.S. 531, 535, 544 (1985), which held that reasonable suspicion was required to detain a suspect at the border for over a day on suspicion that she was smuggling drugs in her alimentary canal.

261. *See* Illinois v. Lidster, 540 U.S. 419, 427 (2004) (concluding that special needs stops to gather information about a fleeing suspect "interfered only minimally" with Fourth Amendment interests when the stops lasted "only a few seconds"); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 448, 451–52 (1990) (concluding that special needs sobriety checkpoints of motorists inflicted only a "minimal" intrusion on Fourth Amendment interests when the average stop lasted 25 seconds); United States v. Place, 462 U.S. 696, 709–710 (1983) (holding that the ninety-minute detention of the suspect's luggage rendered the search unreasonable under the Fourth Amendment).

262. *Place*, 462 U.S. at 709.

263. *See* Terry v. Ohio, 392 U.S. 1, 16 (1968) ("It must be recognized that whenever a police officer accosts an individual and restrains his freedom to walk away, he has 'seized' that person.").

264. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property.").

terminate until the government ceases the search and destroys the copy.[265] Hence, a lengthier search process equals a greater Fourth Amendment intrusion. Consequently, a search similar to the inspection in *Arnold*, which took several hours, would be more permissible than a search that took weeks or months. This model would almost certainly dictate that a forty-nine-day search, such as the one alleged in *House*, must be supported by reasonable suspicion even when the search fulfills a special need.

For the third factor evaluated in calculating the individual's interests, courts should consider whether authorities, when conducting the border search, took the property away from its owner and deprived him or her of possession or use of the item. The Supreme Court has ruled that even in isolation, the removal of a suspect's property from his or her presence constitutes an intrusion on the Fourth Amendment protection against unreasonable seizures.[266] Thus, a prolonged detention of a suspect's laptop, flash drive, cell phone, or other device pursuant to a border search would increase the likelihood that the search is impermissible without individualized suspicion.

This factor may sometimes overlap with the second factor relating to the duration of the search, because a search that lasts longer than several hours would be impractical unless the government detained the property for further inspection and excluded the individual from the facility where they moved the device. But the two factors may be distinct in certain instances. For example, border agents, though still performing an extensive search, could reduce the harm inflicted under this factor by making a copy of the digital information, returning the original device to its owner, and then searching the copy.[267] This procedure would allow the owner to enjoy use of the property during most of the search and would reduce the likelihood of financial hardship in the event that he or she needs the device for work.[268]

During oral arguments in the *Cotterman* case, Chief Judge Alex Kozinski of the Ninth Circuit floated a potential policy argument for prohibiting extend-

265. *See Laptop Searches and Other Violations of Privacy Faced by Americans Returning From Overseas Travel: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. 7 (2008) (statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation) [hereinafter *Hearing*].

266. *See* Soldal v. Cook Cnty., 506 U.S. 56, 72 (1992) (holding that the allegation that respondents dispossessed the petitioner of his trailer home by towing it to another lot was sufficient "to constitute a 'seizure' within the meaning of the Fourth Amendment"); *Place*, 462 U.S. at 709 (holding that agents' transport of the defendant's luggage to a different area and their failure to inform him of how long he would be dispossessed of it exacerbated the Fourth Amendment violation).

267. *See* discussion *supra* Part II.B (noting the ability of software to generate exact copies of digital files, including entire hard drives, which can then be searched).

268. *See* THE CONSTITUTION PROJECT, *supra* note 172, at 5 ("On another occasion, a traveler had his laptop detained for more than a month, requiring him to buy a replacement for his job.").

ed detentions of a suspect's device.[269] Judge Kozinski asked the government's attorney if it was permissible for the state to tell incoming travelers at an airport, "We're very busy, so . . . everyone . . . just leave your computers, iPhones, Kindles, and we'll get them back to you when we're done with them."[270] Under such a scenario, the state could theoretically circumvent the time constraints that usually prevent agents from conducting suspicionless searches against every traveler on the spot by hoarding everyone's devices and taking as long as it needed to search them in offsite labs. Thus, on a macro level, a far greater number of suspicionless searches could occur if the state were allowed to detain the property for an extended period of time. Although such sweeping government action is not prohibited under the existing case law in most jurisdictions, this scenario has fortunately not played out in reality. Under the status quo, in which most courts have not prohibited extended detentions of electronic devices, such detentions still occur in only less than 5 percent of cases.[271] CBP justifies this statistic by explaining that even though the government has the power to detain and search a computer or another digital device for long periods of time, CBP and ICE "[do] not have the resources to conduct searches on every laptop or cell phone that pass[es] through our ports of entry, nor is there a need to do so."[272] Thus, while the government's extended detention of digital property remains particularly harmful to individual suspects, there is not much indication that, systemically, this power has led to a far greater number of suspicionless searches than before. Therefore, because the government has not used its power to detain digital devices as an excuse to indiscriminately impound the property of every traveler crossing the border at a certain location and time, removing the property from the suspect's possession should not automatically trigger a requirement of reasonable suspicion. Instead, while this action should make the search's permissibility less likely, it should still be weighed against the government's interest, and alongside the other individual harms, as part of a totality of the circumstances evaluation.

269. Oral Argument, *supra* note 26, at 20:00–20:19.
270. *Id.*
271. *See* THE CONSTITUTION PROJECT, *supra* note 172, at 10
272. *Hearing*, *supra* note 265, at 59 (statement of Jayson P. Ahern, Deputy Comm'r, U.S. Customs & Border Protection).

### B. Arguments for Categorical Permission of Suspicionless Digital Border Searches

There have typically been two major arguments for the view that suspicionless computer border searches should always be permissible.[273] The first justification is largely philosophical and builds on the longstanding precedent that the Fourth Amendment protects an individual only from government searches and seizures that violate the person's "reasonable expectation of privacy."[274] In order for a court to rule that the individual has a reasonable expectation of privacy at the time of the search, the individual must have a subjective expectation of privacy and society must regard that expectation as normatively reasonable.[275] Since the government's power to search people's belongings "is at its zenith at the international border,"[276] supporters of the view espoused by the *Ickes* court have reasoned that international travelers do not have any expectation of privacy in their electronic devices at a point of entry.[277] Therefore, suspicionless searches of digital property always comport with the Fourth Amendment.

But while travelers may have diminished privacy expectations at the border, they do not have *zero* expectation of privacy in their electronic devices. For example, the vast majority of corporate travel executives responding to one sur-

273. Some scholars have also made a third argument—that treating digital property differently from physical property would create a confusing standard for CBP and ICE officers. *See, e.g.*, Lucadamo, *supra* note 229, at 570 (arguing that requiring reasonable suspicion for searches of laptops would create for border agents "a legal quagmire without a clear set of guidelines of how to inspect, investigate, and search international travelers"). This argument is unpersuasive, however, because border agents already have to navigate varying constitutional thresholds for intrusive searches of the person. *See* 5 LAFAVE, *supra* note 144, § 10.5(b)–(e). Because there is no indication that these requirements have prevented CBP and ICE agents from effectively performing their duties, agents likely will be able to learn and adhere to any new standards for digital searches that courts create under this balancing test.

274. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) ("[T]his Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action.").

275. *See id.* ("This inquiry, as Mr. Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,'—whether, in the words of the *Katz* majority, the individual has shown that 'he seeks to preserve [something] as private.' The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as "reasonable,"'—whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is 'justifiable' under the circumstances." (alteration in original) (citations omitted)).

276. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

277. *See* United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc) (Smith, J., dissenting); Gilmore, *supra* note 206, at 785–86.

vey believed, albeit mistakenly, that their electronic devices could not be searched at the border or at international airports.[278] Furthermore, plaintiffs such as House and Abidor would not file suit for what they perceive as violations of their Fourth Amendment rights if they did not feel that the government violated their privacy. Thus, travelers subjectively expect some degree of privacy over the contents of their digital storage devices. Moreover, for reasons already stated, it is perfectly reasonable to desire freedom from particularly comprehensive and lengthy searches of one's laptop after its detention at the border.[279] If courts have been willing to recognize that such expectations exist with regard to searches of living quarters in vehicles,[280] searches of the person,[281] or destructive searches of one's property,[282] it seems arbitrary to conclude that no similar expectation exists with regard to any other property search.

Second, many commentators argue that a requirement of reasonable suspicion for electronic border searches would undermine the national security interests that CBP and ICE protect.[283] Given that these agencies do not have the resources to search every single traveler, however, they already tend to search only those whom they reasonably suspect of a crime.[284] Perhaps certain criminals would not be caught if courts mandated reasonable suspicion for such searches, but even if such a requirement would significantly hinder the government's ability to apprehend serious criminals who pose a danger to the United States, this argument would still be unpersuasive. While national security concerns have sometimes justified lowering Fourth Amendment standards of reasonableness, they cannot justify eviscerating all protections against searches of massive scope and duration. For example, when the United States conducts electronic surveillance of suspected agents of a foreign entity or government under FISA, it still needs to establish probable cause to believe that the target of

278. *Hearing*, *supra* note 265, at 126–27 (statement of Susan K. Gurley, Executive Director, Association of Corporate Travel Executives) (noting that 81 percent of corporate travel executives who responded to a survey did not realize that electronic devices could be held indefinitely pursuant to a border search).

279. *See* discussion *supra* Part III.B.

280. *See* United States v. Whitted, 541 F.3d 480, 488 (3d Cir. 2008); United States v. Alfonso, 759 F.2d 728, 738 (9th Cir. 1985) ("[E]ven in the context of a border search, the search of private living quarters on a ship should require something more than naked suspicion.").

281. *See supra* note 108.

282. *See supra* note 109.

283. *See, e.g.*, Gilmore, *supra* note 206, at 786–92 (arguing that subjecting computer searches to a "reasonable suspicion" standard would create loopholes that could be exploited by terrorists, drug traffickers, and child pornographers).

284. *See Hearing*, *supra* note 265, at 59 (statement of Jayson P. Ahern, Deputy Comm'r, U.S. Customs & Border Protection) ("When we do conduct a search, it is often premised on facts, circumstances, and inferences which give rise to individualized suspicion.").

the FISA surveillance is an agent of a foreign power.[285] Though there might be a lower expectation of privacy at the border than in the interior of the country, many computer border searches, which reveal not only a person's communications with others but a large amount of other personal information, are arguably far more intrusive than FISA surveillance. Thus, there is no principled reason to adhere to the view of the *Ickes* and *Arnold* courts that any digital border search, regardless of its intrusiveness, is reasonable on balance.[286]

## CONCLUSION

The three-way jurisdictional split on the permissibility of suspicionless border searches of portable electronic devices is problematic not only because of the uncertainty it creates but also because none of the three methods ultimately lays out an ideal path for courts to take in the future. While deciding, ad hoc, whether a digital search requires reasonable suspicion may lead to proper outcomes in individual cases, this approach fails to offer any type of principle that can effectively guide future decisions. Although the clearest guidance would come from categorically permitting suspicionless digital border searches, this approach is incompatible with the realities of the twenty-first-century world. Personal ownership of mobile electronic property that is loaded with highly private information is ubiquitous. Moreover, a search of such an object is likely to be more prolonged and expose more intimate information than a search of a conventional physical container. Additionally, the government's ability to access such a wide variety of information on most computers makes it difficult to ensure that border searches do not trawl for any type of illegal activity committed by the individual, beyond those crimes justified by a special need at the border. Thus, because of these unique characteristics of digital property, all property is not created equal under the border search doctrine.

This Comment's unique, special needs–inspired, reasonableness-balancing test aims to ensure that the border search doctrine does not completely swallow the privacy rights of international travelers. Simultaneously, it also provides organizing principles—a test for determining whether the government is fulfilling a special need at the border and a three-factor test for determining the harms to an individual's Fourth Amendment interests—that courts can use for guidance in future cases. And, unlike any previous method employed by the courts, this model aims to bring digital border searches closer to the general Fourth

285. United States v. Abu-Jihaad, 630 F.3d 102, 130–31 (2d Cir 2010); *In re* Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002).

286. *See supra* note 111 and accompanying text.

Amendment philosophy that searches and seizures not supported by a warrant or probable cause cannot serve broad, nonspecific law enforcement purposes.

Since only a small percentage of border searches of electronic devices involve prolonged detentions and forensic searches[287] like the searches in *Cotterman*, *House*, or *Abidor*, it is unclear whether the proposed reasonableness test would affect the legality of the suspicionless digital border searches that most travelers face. Nonetheless, even if this model impacts only a small minority of individuals searched at the United States' borders each day, courts should not hesitate to subject digital border searches to the greater scrutiny this Comment advocates. For the thousands of travelers who encounter these inspections each year, courts' adoption of this balancing test may help quell their concerns that the United States border has become a "Fourth Amendment-Free Zone."[288]

287. *See supra* note 197 and accompanying text.
288. Kravets, *supra* note 14.