

SUSPICIONLESS LAPTOP SEARCHES UNDER THE BORDER SEARCH DOCTRINE: THE FOURTH AMENDMENT EXCEPTION THAT SWALLOWS YOUR LAPTOP

*Ari B. Fontecchio**

INTRODUCTION

Most American travelers have become familiar with the United States' heightened vigilance at international airports since the terrorist attacks of September 11, 2001. The average American gives little pause when she finds her luggage has been selected for a random search,¹ or when she must leave her bottle of Poland Spring water at the security checkpoint and buy another one on the concourse. For the most part, travelers recognize the necessity of securing the nation's borders at the minimal expense of handing over a bottle of water—trading a small amount of personal privacy for safety. The same cannot be said when a customs agent forces a traveler to hand over her laptop, turns it on, reads her files, copies her data, and stores the computer offsite for an indeterminate amount of time, without *any suspicion* of illegal activity.²

However, a new policy³ published by the Department of Homeland Security (DHS) allows just that, compromising a core privacy protection of the Fourth Amendment. U.S. Customs and Border

* Editor-in-Chief, *Cardozo Law Review*. J.D. Candidate (June 2010), Benjamin N. Cardozo School of Law. Thanks to Professor Ekow Yankah for his encouragement and counsel. Additionally, I am grateful for the superb editing of Brian Sogol and for the direction of Victoria Elman, Scott Danner, and Alison Brill. Special thanks to Meredith Silverman, whose laptop undoubtedly will be searched when we travel together from now on.

¹ *Traveler's Privacy Protection Act of 2008: Statements on Introduced Bills and Joint Resolutions*, 110th Cong. (Sept. 26, 2008) (statement of Senator Russell Feingold introducing S. 3612), available at <http://www.govtrack.us/congress/bill.xpd?bill=s110-3612&tab=speeches> (last visited Sep. 15, 2009) (follow "Statements on Introduced Bills and Resolutions" hyperlink; then follow "Sen. Feingold [D-WI]" hyperlink).

² U.S. Customs and Border Protection, *Policy Regarding Border Search of Information*, § B (July 16, 2008), [hereinafter *CBP Policy*] available at http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf. To date, border agents have searched laptops without a suspicion and have seized them for more than two years without explanation. Odean L. Volker, *Lawyers, Laptops, and the Border*, 72 TEX. B.J. 640, 640-42 (2009).

³ See generally *CBP Policy*.

Protection (CBP), a subsidiary of DHS, published its *Policy Regarding Border Search of Information (CBP Policy)* on July 16, 2008.⁴ The *CBP Policy*⁵ allows customs officers to search, read, copy, retain, and share the private data in one's laptop.⁶ The expansive policy covers numerous electronic storage devices, including computer hard-drives and external data storage units.⁷ It allows CBP agents to read the substance of the files, not simply to glance at them for illegal content.⁸ While the policy purports to provide protection against unreasonable search and seizure⁹ in accordance with the Fourth Amendment,¹⁰ officers may copy and retain one's private files for an indeterminate amount of time¹¹ at an off-site location even "absent individualized suspicion."¹²

Historically, courts based Fourth Amendment analysis on whether an officer had a warrant based upon probable cause.¹³ However, the Supreme Court set forth the modern Fourth Amendment reasonableness-balancing analysis¹⁴ in *Terry v. Ohio*,¹⁵ which provides

⁴ *Id.*

⁵ While suspicionless data and laptop searches at the border are nothing new, publication of the *CBP Policy* is particularly troubling because it represents the government's official approval of a questionable practice that has taken place since September 11, 2001. *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. (2008) [hereinafter *Hearings*], available at <http://www.judiciary.senate.gov/hearings/hearing.cfm?id=3420>.

⁶ *CPB Policy*, *supra* note 2, Introduction. The document "sets forth the legal and policy guidelines within which officers may search, review, retain, and share certain information possessed by individuals who are encountered by [U.S. Customs and Border Protection] at the border . . . [or its] functional equivalent." *Id.*

⁷ *Id.* § A. The scope of a search under the *CBP Policy* extends to "computers, disks, hard drives, and other electronic or digital storage devices." *Id.*

⁸ *Id.* § B. The *CBP Policy* allows CBP agents to "review and analyze the information transported by any individual attempting to enter . . . the United States." *Id.*

⁹ *Id.* § A ("Notwithstanding this law enforcement mission, in the course of every border search, CBP will protect the rights of individuals against unreasonable search and seizure.").

¹⁰ The Fourth Amendment to the U.S. Constitution provides:

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

U.S. CONST. amend. IV.

¹¹ *CPB Policy*, *supra* note 2, § C(1) ("Officers may detain documents and electronic devices, or copies thereof, for a reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location.").

¹² *Id.* § B ("In the course of a border search, and absent individualized suspicion, officers can review and analyze the information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States.").

¹³ The concept of probable cause is discussed *infra* Part I.

¹⁴ This transition from a warrant-based analysis to a reasonableness-balancing-based analysis represents an ongoing debate within Fourth Amendment scholarship: whether the Warrant Clause ("no Warrants shall issue, but upon probable cause") or the Reasonableness Clause ("The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches

that a search is constitutional where the government's interest in preventing crime outweighs the individual's interest in privacy.¹⁶ *Terry* balancing applies to searches performed in the course of traditional¹⁷ law enforcement. Searches performed outside the scope of traditional law enforcement, where the government has a *special* interest—such as preventing drug use in schools, drunk driving on highways, or the entry of terrorists into the U.S.¹⁸—fall within the “special needs doctrine,”¹⁹ where the Court usually finds the government's interest outweighs the individual's. Under *Terry* the government's and the individual's interests enter the balance on even footing, but under special needs balancing, the Court gives the government a nearly insurmountable boost, having pre-determined the existence of a “special” need.²⁰ Almost inevitably, the individual's interests are not meaningfully

and seizures”) is the central requirement of the Fourth Amendment. Those who advocate for the supremacy of the Warrant Requirement argue that there is “a strict (per se) [rule] that insists that searches and seizures always require warrants.” Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 762 (1994) (recognizing the move away from the per se warrant requirement). Adherents of Reasonableness Clause supremacy claim that the “ultimate touchstone” of the Amendment is not warrants, but reasonableness. *Id.* at 768; *see also* JOSHUA DRESSLER & GEORGE C. THOMAS, III, CRIMINAL PROCEDURE: INVESTIGATING CRIME 174-87, 333-37 (3d ed. 2006) [hereinafter DRESSLER & THOMAS] (discussing this ongoing debate).

¹⁵ 392 U.S. 1 (1968).

¹⁶ 2 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE 277-79 (4th ed. 2006) [hereinafter DRESSLER & MICHAELS]. Dressler explains:

Terry provided the impetus, as well as the framework, for a move by the Supreme Court away from the proposition that warrantless searches are per se unreasonable, to the competing view that the appropriate test of police conduct “is not whether it is reasonable to procure a search warrant, but whether the search was reasonable.”

Warrantless police conduct became much easier to justify after *Terry*.

Id. (internal citations omitted).

¹⁷ For the purposes of this brief introduction to the law behind border searches, *traditional* law enforcement includes such activity as performing criminal investigations inside the borders of the U.S. to prosecute criminals involved in murder, arson, theft, rape, and fraud. *See* WAYNE R. LAFAVE ET AL., 2 CRIM. PROC. § 3.9(a)-(i) (3d ed. 2007-2008) (discussing the various types of searches falling within the special needs doctrine).

¹⁸ Such “special needs” searches performed outside the government's traditional law enforcement function include the following: preventing drunk driving by creating sobriety checkpoints, *Mich. Dept. of State Police v. Sitz*, 496 U.S. 444 (1990); maintaining school safety by waiving the warrant requirement for searches in public schools, *New Jersey v. T.L.O.*, 469 U.S. 325 (1985); performing inspections at fire scenes to determine the cause of fire, *Michigan v. Tyler*, 436 U.S. 499 (1978); and maintaining architectural safety standards by performing housing inspections, *Camara v. Municipal Court*, 387 U.S. 523 (1967); *see also* LAFAVE, *supra* note 17, § 3.9(a)-(i) (3d ed. 2007-2008) (discussing the various types of searches falling within the special needs doctrine).

¹⁹ *See generally* *United States v. Flores-Montano*, 541 U.S. 149 (2004). The Supreme Court's analysis in *Camara v. Municipal Court* provides the basis for the theoretical framework for all inspections and regulatory searches under the “special needs doctrine,” such as those at the border. *See* LAFAVE, *supra* note 17, § 3.9(a) (citing *Camara*, 387 U.S. 523, 536-37 (1967) (“Unfortunately, there can be no ready test for determining reasonableness [in the context of special needs analysis] other than by balancing the need to search against the invasion which the search entails.”)).

²⁰ This Note develops this argument at length *infra* Part II.

considered. Nowhere is this lopsided balancing more pronounced than at the United States' borders.

Border searches are one manifestation of the special needs doctrine.²¹ The Supreme Court has found in this context that the government's need to protect the border is so "special" that customs officers can search a traveler and any of his "containers,"²² such as luggage, without a warrant, probable cause, or *any* suspicion of illegal activity. Recently, the Ninth Circuit held that laptops qualify as containers and, therefore, can be searched at the border without any suspicion.²³ This holding ushered in the *CBP Policy* at issue in this Note. Crucial to the Ninth Circuit's holding was its argument that the government's interest at the border is at its "zenith,"²⁴ making it nearly impossible for an individual's privacy interest to prevail *within* the border search and special needs doctrines.²⁵ This Note argues that data searches should be taken *outside* the framework of the lopsided special needs analysis and that the even-footing *Terry* analysis should apply.

Specifically, the starting point of this Note is that the border search and special needs doctrines do not apply to the data inside laptops,

²¹ *United States v. Ramsey*, 431 U.S. 606, 616 (1977) ("[S]earches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."); *see also* LAFAVE, *supra* note 17, § 3.9(f) (discussing the border search doctrine as one manifestation of the special needs doctrine).

²² *Ramsey*, 431 U.S. at 612 n.8 (holding envelopes sent through the U.S. mail are "container[s]" for the purposes of the border search doctrine); *see also* LAFAVE, *supra* note 17, § 3.9(f) (suggesting that under *Ramsey*, "searches of persons and things may be made upon their entry into the country without first obtaining a search warrant and without establishing probable cause or any suspicion at all in the individual case."); *United States v. Arnold*, 533 F.3d 1003, 1007 (9th Cir. 2008), which states:

Courts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment. Searches of the following specific items have been upheld without particularized suspicion: (1) the contents of a traveler's briefcase and luggage; (2) a traveler's "purse, wallet, or pockets;" (3) papers found in containers such as pockets; and (4) pictures, films and other graphic materials.

Id. (summarizing Ninth Circuit case law) (internal citations omitted).

²³ *Arnold*, 533 F.3d 1003.

²⁴ *Id.* at 1007 (citing *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004)).

²⁵ In *Arnold*, for example, the Ninth Circuit rejected defendant's contention that his privacy interest in the data on his laptop was superior to the government's towering interest in protecting its borders:

Arnold argues that . . . reasonable suspicion was required to search his laptop at the border because it is distinguishable from other containers of documents based on its ability to store greater amounts of information and its unique role in modern life. . . . '[L]aptop computers are fundamentally different from traditional closed containers,' . . . [because] a laptop's capacity allows for the storage of personal documents in an amount equivalent to that stored in one's home. He argues that a laptop is like the 'human mind' because of its ability to record ideas, e-mail, internet chats and web-surfing habits.

Id. at 1006.

because data travels electronically via cyberspace,²⁶ not through the United States' physical borders such as airports and highways.²⁷ The government has no *special* need to search data at these physical borders separate and apart from searching data in computers already inside the country.

At its core, this Note argues that suspicionless data searches actually compromise border security by allowing officers to engage in time-consuming data searches²⁸ instead of preventing the entry of weapons that can cause immediate harm. Since such data searches hurt rather than help to achieve border security, the government's interest in performing *suspicionless* data searches at the border is not actually at its zenith, and the lopsided special needs balancing analysis should not apply. Instead, even-footing *Terry* reasonableness-balancing should be used to evaluate whether a data search at the border violates the Fourth Amendment. On balance, an individual's privacy interests should prevail. Consequently, the *CBP Policy* allowing suspicionless searches of laptop data violates the Fourth Amendment.

Part I of this Note sets forth the legal background of the border search and special needs doctrines from which the *CBP Policy* has grown. Subsequent Parts of this Note establish and balance the government's and the individual's competing interests. Part II explains why the special needs doctrine does not apply to searching a computer's data at the United States' borders.²⁹ It follows that the government's

²⁶ In a recently published Note, Rasha Alzahabi argues that the rationale behind the border search doctrine does not apply to the information inside a laptop because "[t]he information saved on a laptop can be transported into our country electronically, regardless of whether the traveler or the laptop crosses the border." Rasha Alzahabi, *Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers*, 41 IND. L. REV. 161, 175 (2008). This Note adopts this argument as its starting point, elaborates on the argument, and adds new analysis to both sides of the balance between the government's and the individual's interests.

²⁷ Airports, highways, and waterways are considered to be the "functional equivalents" of the nation's physical border. The border search and special needs doctrines extend to all such functional equivalents. DRESSLER & THOMAS, *supra* note 14, at 414.

²⁸ One recent case involved a suspicionless data search that lasted four days, tying up numerous officers to uncover contraband. *United States v. Cotterman*, No. 07-1207, 2009 WL 465028, at *3 (D. Ariz. Feb. 24, 2009). One officer actually drove the computer to a secondary search location 170 miles from the point of seizure. *Id.*

²⁹ In a recently published article, Lester M. Paredes III proceeds from a similar premise: that requiring a higher level of suspicion for border searches is likely to have "little or no effect on terrorist activity. Terrorists can email their communications and be protected by a probable cause requirement." Lester M. Paredes, III, *The Travelers' Privacy Protection Act: Be Reasonable with My Private Information and Expensive Equipment*, 45 No. 1 CRIM. L. BULL. 1, 15 (Jan.-Feb. 2009). Additionally, Paredes argues that extending suspicionless laptop searches to places other than the border would make it so "no person, home or computer wherever found would be safe from suspicionless searches." *Id.* This Note also argues that the government's interest is reduced and an individual's interest is heightened when it comes to data searches at the border, but analyzes both the government's and the individual's interests in a different way. On the side of the government, this Note argues that suspicionless searches at the border actually decrease

interest is not at its zenith. Part III addresses the heightened privacy concerns of an individual whose data has been searched. This Part addresses privacy concerns already set forth by scholars and establishes a new one: the increasing nexus between computers and the interior of the human body, caused by medical advancements such as diabetes-related glucose monitors placed beneath the skin and viewed from a laptop. Finally, Part IV proposes that the government should require a customs agent to have “one good reason”³⁰ before performing an intrusive data search at the border. This standard would require an officer to have more than no suspicion yet less than a reasonable suspicion³¹ or probable cause³² to search the data inside one’s laptop. This solution strikes an appropriate balance between the government’s need to protect its borders and a traveler’s privacy interest in her data.

I. LEGAL BACKGROUND: THE BORDER SEARCH AND SPECIAL NEEDS DOCTRINES

A. *Transition to a New Fourth Amendment Analysis: Terry Reasonableness-Balancing*

At its core, the Fourth Amendment protects individual privacy against certain intrusions by the government.³³ Traditionally, such

border security and frustrate the government’s special need to protect the border by allowing CBP agents to waste their resources performing time-consuming data searches. Suspicionless searches in other special situations—such as sobriety checkpoints and school safety searches—actually achieve the government’s interests, arguably warranting a lower level of suspicion. On the side of the individual, this Note focuses on the nexus between the interior of the human body and the data inside a laptop. In effect, technological advances in the medical field may turn the data in one’s computer into a virtual reflection of the *interior* of one’s body.

³⁰ Briefly, the “one good reason” standard is meant to constitute a level of suspicion above the “no suspicion” standard in the *CBP Policy* and below the “reasonable suspicion standard” set forth in *Terry v. Ohio*, which justifies stopping and frisking a criminal suspect on the street. 392 U.S. 1 (1968). As a reference, all three of these standards—no suspicion, one good reason, and reasonable suspicion—all fall below the “probable cause” standard set forth in *Illinois v. Gates*. 462 U.S. 213 (1983). Each of these standards is discussed in detail *infra* Part I.

³¹ Notably, others have argued that border search policies with respect to laptop computers should require a *reasonable* suspicion. Recently, Senator Russell Feingold introduced such a proposal to the Senate. Traveler’s Privacy Protection Act, S. 3612, 110th Cong. § 4 (as introduced in Senate, Sept. 26, 2008). If passed, the Travelers’ Privacy Protection Act would require border agents to have a *reasonable suspicion* before searching a traveler’s electronic devices. See *Hearings, supra* note 1, testimony of Sen. Russell Feingold.

³² This constitutional standard is discussed *infra* note 35.

³³ *Katz v. United States*, 389 U.S. 347, 350 (1967) (“[The Fourth] Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.”). Additionally, it is important to note that the Fourth Amendment does not create a “general constitutional ‘right to privacy.’” *Id.* “The Fourth Amendment protects privacy only to the extent that it prohibits unreasonable searches and seizures of ‘persons, houses, papers, and effects.’” *Id.* at 371 (Black, J., dissenting).

intrusions required a warrant³⁴ based on probable cause³⁵ to prevent “unreasonable searches and seizures.”³⁶ Under this per se warrant rule, a search was reasonable and, therefore, Constitutional³⁷ where the warrant was properly issued.³⁸

In 1968, when the Court decided *Terry v. Ohio*,³⁹ it set forth a sea change in Fourth Amendment analysis. Scholars have interpreted *Terry* as abandoning the per se warrant rule in favor of an analysis whose hallmark is reasonableness-balancing.⁴⁰ *Terry* balancing applies in situations where an officer with less than probable cause intrudes on

³⁴ See *Groh v. Ramirez*, 540 U.S. 551, 572-73 (2004) (“[O]ur cases stand for the illuminating proposition that warrantless searches are per se unreasonable, except, of course, when they are not.”) (Thomas, J., dissenting); see also DRESSLER & MICHAELS, *supra* note 16, at 277-79:

The Fourth Amendment was once considered a monolith. “Probable cause” had a single meaning, and “searches” and “seizures” were all-or-nothing concepts. The monolith was cracked by the Supreme Court in *Camara v. Municipal Court*. In *Camara*, the justices recognized a different form of “probable cause,” applicable to administrative-search cases, that does not require individualized suspicion and which is based on the general Fourth Amendment standard of “reasonableness.” To determine “reasonableness,” the *Camara* Court invoked a balancing test, in which the individual’s and society’s interests in a given type of administrative search were weighed against each other.

Id.; Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of Camara and Terry*, 72 MINN. L. REV. 386 (1988) (“Prior to *Camara*, Fourth Amendment analysis had a relatively high amount of predictability: the Court presumed that a warrant based on probable cause was required before the police could perform a search or arrest.”).

³⁵ The definition of probable cause has been explained as follows:

“Probable cause to arrest ‘exists where “the facts and circumstances within [the officers’] knowledge and of which they [have] reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that’ *an offense has been or is being committed*’ by the person to be arrested. . . . The same definition applies to ‘probable cause to search,’ except that the italicized language is replaced with ‘evidence subject to seizure will be found in the place to be searched.’”

DRESSLER & THOMAS, *supra* note 14, at 132 (internal citations omitted). Probable cause to search is a flexible, practical, common-sense determination about human behavior made by officers in the field. See *Illinois v. Gates*, 462 U.S. 213, 230-32 (1983). Generally, an officer looks to the “totality-of-circumstances” from his perspective to determine whether crime is afoot. *Id.* at 252. “[T]he evidence thus collected must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement.” *Id.* at 232. Additionally, probable cause requires a higher showing than a mere reasonable suspicion.

³⁶ U.S. CONST. amend IV.

³⁷ See Sundby, *supra* note 34, at 386-89.

³⁸ *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326-27 (1979) (holding unconstitutional under the per se warrant rule an officer’s search for illegal videotapes pursuant to an overly general, invalid warrant).

³⁹ 392 U.S. 1 (1968).

⁴⁰ See Sundby, *supra* note 34, at 385. Whether this sea change represents the Supreme Court’s official position is a live debate. See *supra* note 14 and accompanying text. For the purpose of this Note, where the special needs and border search doctrines are at issue, a reasonableness-balancing approach is undoubtedly the relevant mode of analysis. See *Flores-Montano*, 541 U.S. 149, 152-53 (2004) (“Time and again, we have stated that ‘searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are *reasonable* simply by virtue of the fact that they occur at the border.’”) (internal citations omitted) (emphasis added).

individual privacy. The Court's initial inquiry is whether the government's interest in preventing crime is superior to the individual's interest in personal privacy⁴¹ in the totality of the circumstances.⁴² Where the government's interest is superior, the search is reasonable and constitutional.⁴³

Critically, before the Court engages in *Terry* balancing, the government's and individual's interests begin *on even footing*. Neither the officer nor the individual has an automatic advantage before the Court considers the totality. In *Terry* the Court began by acknowledging the government's and the individual's inherently competing interests.⁴⁴ Then, the Court considered the specifics of the particular encounter,⁴⁵ finding the officer's interests were superior and upholding as reasonable a "stop and frisk" for weapons without probable cause.⁴⁶

In contrast to *Terry* balancing where the interests begin on even footing, the Court also balances interests in "special" contexts, where the government enters the balance with a distinct advantage. The Court has called this lopsided balancing the "special needs doctrine."⁴⁷

⁴¹ *Terry v. Ohio*, 392 U.S. 1 (1968). The Court set forth the *Terry* reasonableness-balancing test as follows: First, the Court evaluated the "governmental interest" in crime prevention and detection; then, it considered "the nature and quality of the intrusion on individual rights;" finally, the Court "balanc[ed] the need to search (or seize) against the invasion the search (or seizure) entails." *Id.* at 20-24. The Court suggested it should engage in this kind of balancing where "probable cause to arrest for crime is lacking." *Id.*

⁴² *Id.* at 22-25. In *Terry*, an officer witnessed a group of youths "hover[ing] about a street corner for an extended period of time," repeatedly looking into a store over twenty-four times. The officer's thirty years of experience with street crimes told him the youths would likely be armed, so in the interest of crime prevention and officer safety, the Court found the officer's patting down of the suspect to look for weapons was constitutional under the totality of circumstances despite the fact the officer's level of suspicion did not give rise to probable cause. *Id.* at 29-31.

⁴³ Where the individual's interest is superior, a search is unreasonable, violating the Fourth Amendment. *See id.*

⁴⁴ The Court found an officer has an inherent interest in crime prevention and personal safety in the course of a dangerous job. *Id.* at 22-24. An individual has an interest in "cherished personal security" and in being free from an annoying, frightening, and humiliating experience. *Id.* at 25.

⁴⁵ In the case, an experienced officer believed a group of youths may have possessed weapons based on the way they were "casing a job" at a particular store. *Id.* at 6.

⁴⁶ *Id.* at 30.

⁴⁷ *City of Indianapolis v. Edmond*, 531 U.S. 32, 54 (2000) (Rehnquist, C.J., dissenting) ("The 'special needs' doctrine, which has been used to uphold certain suspicionless searches performed for reasons unrelated to law enforcement, is an exception to the general rule that a search must be based on individualized suspicion of wrongdoing."); *New Jersey v. T.L.O.*, 469 U.S. 325, 351, (1985) (Blackmun, J., concurring) ("Only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers."); *see also* LAFAVE, *supra* note 17, § 3.9(a). In his treatise on criminal procedure, LaFave discusses the "special needs doctrine" at issue in this Note:

Some of the [special needs] practices, such as the examination of the effects of persons entering the country from abroad, have been followed for many years and have rather

B. *The Special Needs Doctrine*⁴⁸

As in *Terry*, the special needs doctrine allows the government to perform searches without obtaining a warrant or showing probable cause.⁴⁹ The purpose of special needs searches is to solve unique problems in particular contexts, such as eliminating drugs from school zones and preventing drunk driving on U.S. highways.⁵⁰ In such contexts, the Court has used a unique balancing analysis, where the government has a distinct advantage over an individual's interests *from the outset*, before the Court considers the totality of the circumstances.

The Court set forth this special needs analysis⁵¹ in *Camara v. Municipal Court*,⁵² wherein it purported to balance the government's interest in achieving its "special" need against the individual's interest

strong historical credentials, while others, such as the airport hijacker detection screening process, are rather recent innovations undertaken in an effort to respond to new problems. However, [special needs searches] all have this in common: it is generally assumed that the problems to which they are addressed could not be dealt with adequately under the usual Fourth Amendment restraints and that consequently the practices must be judged by somewhat different standards.

Id.

⁴⁸ *Camara*, 387 U.S. at 538 (reasoning that in the special context of health and safety regulation, an inspecting officer does not "need [to] show the same kind of proof . . . to obtain a warrant" as an officer performing a criminal investigation). See also DRESSLER & THOMAS, *supra* note 14, at 413-14 (discussing the "birth" of the special needs doctrine). Dressler suggests that the first use of the term "special needs" doctrine is not in *Camara* but in *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). In *T.L.O.* a public school principal searched and seized a girl's purse after he heard she was smoking on school grounds. After finding smoking paraphernalia, he searched her entire purse and found evidence she was selling marijuana. After balancing the school's need to prevent drug sales on its premises against the individual's privacy interest in her containers (such as her purse), the Court upheld the search. *Id.* at 347-48. See also DRESSLER & THOMAS, *supra* note 14, at 413-14 (summarizing *T.L.O.*). Later the special needs doctrine was extended into additional contexts: preventing drunk driving by creating sobriety checkpoints, *Mich. Dept. of State Police v. Sitz*, 496 U.S. 444 (1990); performing inspections at fire scenes to determine the cause of fire, *Michigan v. Tyler*, 436 U.S. 499 (1978); and maintaining architectural safety standards by performing housing inspections, *Camara v. Municipal Court*, 387 U.S. 523 (1967); see also LAFAVE, *supra* note 17, § 3.9(a)-(i) (discussing the various types of searches falling within the special needs doctrine).

⁴⁹ *Camara v. Municipal Court*, 387 U.S. 523 (1967). See also LAFAVE, *supra* note 17, § 3.9(a) (discussing, generally, the theoretical framework of the special needs doctrine).

⁵⁰ See LAFAVE, *supra* note 17, § 3.9(a)-(i). LaFave provides several examples of special needs searches, including housing, business, welfare and fire inspections, *id.* at § 3.9(b)-(e), vehicle regulation, *id.* at § 3.9(g), prison searches, *id.* at § 3.9(i), student searches for drugs and weapons in schools, *id.* at § 3.9(k), and drug testing for public employees, *id.* at § 3.9(l). Such searches are evaluated under the *reasonableness* or *balancing* standard set forth in *Camara v. Municipal Court*, 387 U.S. 523, 536-37 (1967). See LAFAVE, *supra* note 17, § 3.9(a). The reasonableness balancing analysis set forth in *Camara* is the focus of the discussion in this section *infra*.

⁵¹ LAFAVE, *supra* note 17, § 3.9(a).

⁵² 387 U.S. 523, 536-37 (1967).

in privacy⁵³ by using a three-pronged test. First, the Court determined whether the practice was historically accepted;⁵⁴ second, it considered whether the government could have satisfied its needs in another way that infringed less on individual rights;⁵⁵ and third, it examined the magnitude of infringement in the present case.⁵⁶ Over time the second prong dropped away, effectively reducing the protection of individual rights.⁵⁷ This resulted in the lopsided special needs balancing test the Court uses today.

In *Camara* in 1967 the Court evaluated the reasonableness of a housing inspection practice, where inspectors, without probable cause, entered apartments to achieve the special need of architectural and electrical safety in city buildings.⁵⁸ In its analysis, the Court balanced “the need to search against the invasion which the search entails.”⁵⁹

Subsequent special needs cases demonstrate the Court’s movement away from the second prong of *Camara*, determining whether there is

⁵³ See *infra* notes 59-56 and accompanying text.

⁵⁴ *Camara*, 387 U.S. at 537 (“[Search] programs have a long history of judicial and public acceptance.”). On this *first* prong the Court found the practice had strong roots in the community. *Id.* Specifically, the Court found “[t]ime and experience have forcefully taught that the power to inspect dwelling places, either as a matter of systematic area-by-area search or, as here, to treat a specific problem, is of indispensable importance to the maintenance of community health.” *Id.*

⁵⁵ *Id.* (“[I]t is doubtful that any other technique . . . would achieve acceptable results.”). This *second* prong has also been called a “least restrictive means test.” See LAFAVE, *supra* note 17, § 3.9(i). Here, the Court evaluated whether there was a means of checking for dangerous structural flaws in the building less restrictive on individual privacy than actually entering the apartment. *Camara*, 387 U.S. at 537. The Court found entering the apartment was the only way to check for problems such as dangerous faulty wiring. *Id.* The Court stated: “[m]any such conditions—faulty wiring is an obvious example—are not observable from outside the building and indeed may not be apparent to the inexpert occupant himself.” *Id.*

⁵⁶ *Id.* On this *third* prong, the Court found that since apartment safety inspections did not target specific occupants, the search involved a limited invasion of personal privacy. *Id.* Balancing these competing interests, the Court found the housing inspections were reasonable and did not violate the Fourth Amendment. See also LAFAVE, *supra* note 17, § 3.9(a) (discussing the Court’s balancing analysis in *Camara*, 387 U.S. at 536-37).

⁵⁷ See *infra* notes 60-67 and accompanying text.

⁵⁸ *Camara*, 387 U.S. 523.

⁵⁹ *Id.* at 537. An apt illustration is the case of *Camara* itself, where the Court found it would have been unconstitutional for a housing inspector to enter the defendant’s premises without an administrative “warrant,” which the inspector could have obtained without even showing any particularized suspicion of housing code violations. *Id.* at 534. See also DRESSLER & THOMAS, *supra* note 14, at 412-13 (discussing the holding in *Camara*). In *Camara* there was no emergency requiring immediate entry into the defendant’s apartment. *Camara*, 387 U.S. at 539. Therefore, immediate inspection was *non-essential* to the special governmental need of ensuring housing safety for the public in general. *Id.* at 540. The Court’s decision turned on the inspector’s ability to readily obtain an inspection “warrant” by filling out a few forms. *Id.* The Court’s reasonableness balancing analysis led to the protection of an individual’s privacy where the potential invasion was non-essential to the government’s objective. *Id.* Unfortunately, the Court has moved away from the three-pronged analysis in *Camara* in favor of the simply balancing the government’s interest against the individual’s. See, e.g., *Flores-Montano*, 541 U.S. 149, 152-54 (2004) (exemplifying the more simplistic balancing analysis, discussed in greater detail *infra* Part I.C); see generally LAFAVE, *supra* note 17, § 3.9.

another less privacy-infringing way to achieve the government's special need. This shift, evident in *Vernonia School District v. Acton*⁶⁰ has led to under-protecting individual rights. There, the Court upheld a suspicionless search of a student's book-bag, because the school had a special interest in eliminating its student drug problem.⁶¹ In *Vernonia* the Court did consider, yet quickly rejected, a less privacy-restrictive alternative, encouraging parents to police the problem.⁶² In doing so, the Court suggested it has never been *required* to search for a less privacy-restrictive alternative, a sentiment creating an advantage for the government before the balancing test begins.

This predetermined government advantage, rooted in the Court's shift away from *Camara*'s second prong, is evident in numerous other special needs contexts, including searches at fire scenes,⁶³ drunk driving checkpoints,⁶⁴ and places of federal employment.⁶⁵ Critical to the purpose of this Note is recognizing that, if the Court moved away from *Camara*'s second prong in those special needs contexts, it has

⁶⁰ *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995).

⁶¹ *Id.* at 663.

⁶² *Id.* In rejecting this less privacy-infringing alternative, the Court suggested it has never been *required* to look for the least restrictive alternative:

As to the efficacy of this means for addressing the problem: It seems to us self-evident that a drug problem largely fueled by the "role model" effect of athletes' drug use, and of particular danger to athletes, is effectively addressed by making sure that athletes do not use drugs. Respondents argue that a "less intrusive means to the same end" was available, namely, "drug testing on suspicion of drug use." We have repeatedly refused to declare that only the "least intrusive" search practicable can be reasonable under the Fourth Amendment. Respondents' alternative entails substantial difficulties—if it is indeed practicable at all.

Id. at 663 (internal citations omitted).

⁶³ *Michigan v. Tyler*, 436 U.S. 499, 511 (1978) (engaging in reasonableness-balancing to hold no warrant was required to enter a burning building no matter what level of individual privacy existed in the premises). In *Tyler*, the Court omitted any meaningful consideration of individual rights by failing to consider prong two of *Camara*. Specifically, defendant argued that it would have been less intrusive on his individual privacy interests if the firefighter had simply put out the fire, then left the apartment rather than staying and performing a full search of the entire premises. *Id.* at 509-10. Essentially, the Court quickly rejected this less restrictive method as a means incapable of satisfying the government's interest in putting out the fire, and preventing more fires like it in the future. *Id.*

⁶⁴ *Mich. Dept. of State Police v. Sitz*, 496 U.S. 444, 455 (1990) (engaging in special needs balancing analysis where the government's need from the outset to prevent drunk driving trumped an individual's right to travel on a road free from police stops at fixed checkpoints). Here, the Court fails even to cite to *Camara*, relying instead on subsequent special needs cases where the Court abandoned *Camara*'s second prong altogether. *Id.* 450-52. *But see* *Delaware v. Prouse*, 440 U.S. 648, 663 (1979) (holding that outside the context of a drunk-driving checkpoint, officers need a reasonable suspicion to stop a driver and demand his license).

⁶⁵ *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989). Although citing to *Camara*, the Court almost entirely omitted the prong-two inquiry. *Id.* at 667-69. Here, the government's special need was to ensure federal border search agents were not addicted to drugs, so the government subjected its employees to mandatory urine tests without any individualized suspicion. While the Court quickly addressed a less-restrictive alternative to these suspicionless searches—namely, requiring a warrant—it immediately rejected the idea. *Id.* at 667.

completely abandoned this prong in the context of border searches,⁶⁶ where the Court has held the government's interest is at its "zenith."⁶⁷

C. *The Border Search Doctrine: A Manifestation of the Special Needs Doctrine*

In the context of border searches, the government has a special need to inspect people and "effects"⁶⁸ entering the U.S. from abroad to protect the United States' borders. Such searches, like others under the special needs doctrine, are "distinct from ordinary law enforcement,"⁶⁹ allowing an officer to perform a search without a warrant, probable cause, or any individualized suspicion of wrongdoing.⁷⁰ Therefore, at the border, the Supreme Court has held that the government can search one's property—including vehicles, suitcases, and other traditional containers⁷¹—without any suspicion whatsoever.⁷² To determine the

⁶⁶ Alternatively to the core argument in this Note—that data searches should be analyzed entirely *outside* the special needs doctrine, which does not apply to data at the border—this Note suggests that if the Court does find the special needs doctrine applies, it should at least use all three prongs of *Camara*, not the lopsided special needs balancing analysis that has emerged in its wake. At least in *Camara*, the Court meaningfully considered less restrictive means (prong two) of achieving the government's special needs. This consideration promotes judicial integrity by providing a defendant with a way of arguing his case. Under the lopsided special needs analysis that has emerged since *Camara*, and especially in its manifestation at the border—as in *Flores-Montano*, 541 U.S. 149 (2004) and *Arnold*, 533 F.3d 1003 (9th Cir. 2008), *infra*—defendants' arguments become almost hopeless, lulling advocates into abandoning privacy arguments in the context of border searches. This is counterintuitive, because privacy is a core Fourth Amendment interest and *should* be considered in any context.

⁶⁷ *Flores-Montano*, 541 U.S. 149, 152 (2004).

⁶⁸ One's effects are the objects she carries into the country. The dictionary defines "effects" as one's goods, movables, or personal property. See Dictionary.com, <http://dictionary.reference.com/browse/effects>.

⁶⁹ LAFAVE, *supra* note 17, § 3.9(a) (citing *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995)).

⁷⁰ *Ramsey*, 431 U.S. at 619:

Border searches . . . from before the adoption of the Fourth Amendment, have been considered to be "reasonable" by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless "reasonable" has a history as old as the Fourth Amendment itself. We reaffirm it now.

(internal citations omitted). See also DRESSLER & THOMAS, *supra* note 14, at 414 ("At the border and its functional equivalent (*e.g.*, at an airport where an international flight arrives), a person may be stopped (seized) and her belongings searched without a warrant and in the absence of individualized suspicion of wrongdoing.") (citing *Ramsey*).

⁷¹ This Note uses the term "traditional containers" as distinct from laptops and other electronic devices that contain data. Traditional containers, for the purposes of this Note, include such things as wallets, bags, suitcases, or any other container that carries physical items (such as clothing, papers, narcotics, and weapons). Data itself is not physical, making its container different from all others.

constitutionality of a search, the Court simply asks whether the search is “routine.”⁷³ If it finds the search is routine, then it is reasonable, and no suspicion is required. The default is that a border search is routine unless it falls within a limited set of non-routine categories such as x-ray searches, strip searches, or alimentary canal searches,⁷⁴ where the Court requires some level of suspicion before the search can be found constitutional.⁷⁵

The Court’s most recent statement on the border search doctrine was in *United States v. Flores-Montano* in 2004,⁷⁶ where it held that dismantling the gas tank of defendant’s vehicle was routine⁷⁷ and constitutional despite the officer’s lack of a reasonable suspicion.⁷⁸ The Court reasoned that, in any border search, the “government’s interest in preventing the entry of unwanted persons and effects is at its zenith.”⁷⁹ The Court engaged in a balancing analysis that omitted consideration of less privacy-infringing alternatives to automobile searches at the border,⁸⁰ finding the government’s immense interest in border protection easily prevailed over an individual’s privacy interest in personal property.⁸¹

Essentially, the Court created a bright line rule: examining “persons and property”⁸² at the border without a particularized suspicion is reasonable with two exceptions. First, the search cannot be “highly intrusive,” and second, it cannot be carried out in a “particularly

⁷² See *Flores-Montano*, 541 U.S. 149.

⁷³ *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

⁷⁴ *Flores-Montano*, 541 U.S. at 152 (citing *Montoya de Hernandez*, 473 U.S. at 538).

⁷⁵ The question of whether laptop searches are routine is discussed *infra* Part III.

⁷⁶ *Flores-Montano*, 541 U.S. 149.

⁷⁷ In the context of border searches, reasonableness depends on whether the Court considers the search “routine,” such as with a traditional container or “nonroutine,” such as with invasive alimentary canal searches in which an officer actually enters a person’s body. See *id.* at 152-53.

⁷⁸ *Id.* at 150.

⁷⁹ *Id.* at 152.

⁸⁰ The Court began its analysis by asking whether the search in question has a long history of acceptance by the public and the courts, citing *Camara*. Then, citing *Ramsey*, it affirmed that border searches have an “impressive historical pedigree.” *Flores-Montano*, 541 U.S. at 152-53 (“It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity.”). The Court continued its analysis by citing statistics illustrating the government’s immense interest in performing border searches to detect contraband. *Id.* at 153-54. Its statistics demonstrated that border searches are an effective means of preventing the entry of contraband in the U.S. See *id.* Finally, the Court considered the level of intrusiveness of dismantling a passenger’s gas tank, which the Court concluded was minimal, as it would be in any case of personal property. *Id.* at 154. To support this proposition, the Chief Justice cited *Carroll v. United States*, 267 U.S. 132, 154 (1925), which held that a passenger entering the U.S. is aware he will be stopped and asked for identification, and therefore his reasonable expectation of privacy diminishes at the border.

⁸¹ *Flores-Montano*, 541 U.S. at 155. The Court provided a summary of its analysis: “While the interference with a motorist’s possessory interest is not insignificant when the Government removes, disassembles, and reassembles his gas tank, it nevertheless is justified by the Government’s paramount interest in protecting the border.” *Id.*

⁸² *Id.* at 152-53.

offensive manner.”⁸³ Neither exception applied in *Flores-Montano*, setting forth a rule whereby almost nothing but a search of the human body would require any level of suspicion. The Court explicitly rejected “complex balancing tests,” demonstrating there was no room for a *Camara* restrictiveness inquiry at the border,⁸⁴ which gave the government an almost insurmountable advantage in this context. In the three cases *infra*, which extend the doctrine to the data inside laptops, it becomes clear that almost no privacy argument, short of invading the body itself, will prevail over the government’s interest, because the Court engages in lopsided special needs balancing.

D. *Extending the Border Search Doctrine to the Data Inside Laptop Computers*⁸⁵

Three key cases demonstrate how federal circuit Courts of Appeals have extended the *Flores-Montano* border search rule to data inside laptop computers, creating a powerful advantage for the government. In 2004, shortly after the Supreme Court’s decision in *Flores-Montano*, the Fourth Circuit decided *United States v. Ickes*,⁸⁶ in which a border agent searched defendant’s van and laptop as he crossed from Canada to the U.S. and found child pornography.⁸⁷ Critically, in *Ickes* the computer search occurred after the border search officer established clearly articulable reasons⁸⁸ to believe the computer’s data contained contraband.⁸⁹ Citing *Flores-Montano* the Fourth Circuit considered the government’s interest superior at the outset and found for the government.⁹⁰

⁸³ *Id.* at 152-54. Seemingly, both standards require a strong showing by the defendant. In this case, for example, the Court suggests that hammering one’s gas tank out of his car is reasonable for the purpose of the border search doctrine. *Id.* at 151.

⁸⁴ *Id.* at 152 (“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.”).

⁸⁵ To date, the Supreme Court has not ruled on whether the border search doctrine allows the suspicionless search of laptops and their data.

⁸⁶ See generally *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005).

⁸⁷ *Id.* at 502-03. Here, the officer’s search actually occurred in two stages. First, the officer performed a suspicionless border search of the defendant’s van where he found marijuana, an outstanding warrant, and nude photographs of minors. Second, with his suspicions raised, the officer thoroughly searched the defendant’s computer, where he found data containing additional child pornography. *Id.*

⁸⁸ The officer’s suspicion was based on finding drug paraphernalia and nude pictures of young boys. *Id.*

⁸⁹ *Id.* at 502.

⁹⁰ First, the Fourth Circuit deferred to longstanding historical acceptance of the border search doctrine, justifying the government’s “overriding interest in securing the safety of its citizens [by preventing] ‘the introduction of contraband into this country.’” *Id.* at 506 (internal citation omitted). The court continued:

The border search doctrine is not a recent development in the law. The “longstanding

In 2006, in *United States v. Romm*,⁹¹ the Ninth Circuit followed the Fourth and held laptop searches without probable cause are constitutional under the border search doctrine⁹² when they occur at international airports inside the U.S.⁹³ Like the Fourth Circuit in *Ickes*, the Ninth Circuit in *Romm* left open the question of whether *suspicionless* laptop searches at the border are constitutional.⁹⁴ Using a

recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself." *United States v. Ramsey*, 431 U.S. 606 (1977). In fact, the same Congress which proposed the Fourth Amendment to state legislatures also enacted the first far-reaching customs statute in 1790. *Id.* at 616. Thus, since the birth of our country, customs officials have wielded broad authority to search the belongings of would-be entrants without obtaining a warrant and without establishing probable cause. *Id.*; see also *Montoya de Hernandez*, 473 U.S. 531, 538 (1985); *United States v. Villamonte-Marquez*, 462 U.S. 579, 584-85 (1983).

Id. at 505-06 (internal citations modified). Finally, when the court moved to the individual interest prong of the special needs balancing analysis, it found a traveler has a decreased expectation of privacy when he crosses a U.S. border. *Id.* at 506 (finding a passenger's privacy interest upon entering the U.S. is "substantially lessened"). This diminished expectation applies to his vehicle and any containers inside it. *Id.* at 506-08. Finally, the court held that the aggregate impact on the privacy interest of all travelers whose computers are searched at the border is decreased further because officers have neither the resources nor the time to search the contents of every computer that comes across the border. *Id.* at 507 (rejecting as "far-fetched" defendant's argument that "any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer hard drive" because "[c]ustoms agents have neither the time nor the resources to search the contents of every computer").

⁹¹ *United States v. Romm*, 455 F.3d 990, 994 (9th Cir. 2006).

⁹² *Id.* at 1006.

⁹³ In his treatise on criminal procedure, Prof. LaFave explains how the border search exception extends to the "functional equivalents" of the borders of the U.S., which include international airports inside the country:

[R]outine border searches may be made at the border when entry is by land from Canada or Mexico, at a place where a ship finally docks after coming from foreign waters, or a place where aircraft land at the end of an international flight, and there is also authority that they may be conducted inland at a "functional equivalent of the border" [T]hese routine searches can be justified by resort [sic] to the *Camara* balancing analysis, as there is a "vital national interest in preventing illegal entry and smuggling" and the searches are a "limited invasion" in the sense that they are directed at a morally neutral class of persons who have it within their power to determine the time and place of the search.

LAFAVE, *supra* note 17, § 3.9(f).

⁹⁴ In this case Canadian officers reported to U.S. officers the presence of child pornography on the defendant's laptop before the U.S. agents performed their search. When Romm attempted to enter British Columbia, officers from the Canada Border Search Agency discovered he had a criminal history. *Romm*, 455 F.3d at 997 n.11 (9th Cir. 2006). When they alerted Romm they would be searching the contents of his laptop, the defendant admitted, "That's it. My life's over." *Id.* Upon Romm's admission, the Canadian officers refused the defendant entry into Canada, and alerted their U.S. counterparts at Seattle-Tacoma Airport that Romm was on his way back to the U.S. When Romm arrived, Agent Macho searched the defendant's laptop, finding ten images of child pornography. A secondary search by Detective Luckie uncovered additional child pornography hidden in the computer's cache memory. *Id.* at 994. The Ninth Circuit deferred the question whether to allow suspicionless laptop searches under the border search doctrine. *Id.* at 997 n.11 ("Since this issue is not before us here, however, we need not decide whether the search of Romm's laptop was 'non-routine' and if so, whether it was supported by reasonable

balancing analysis nearly identical to the one used by the Fourth Circuit, the Ninth Circuit found the government's interest in protecting its borders outweighed the invasion of the defendant's privacy.⁹⁵ In dicta, the Ninth Circuit went further, suggesting it would find even a *suspicionless* laptop search constitutional under the border search doctrine, and that the search at issue was routine, reasonable, and constitutional.⁹⁶

E. *The Ninth Circuit's Over-Expansion of the Border Search Doctrine in Arnold*

In 2008, in *United States v. Arnold*, the Ninth Circuit explicitly held that a suspicionless laptop search was routine and reasonable under the border search doctrine.⁹⁷ Specifically, the court held as constitutional a search in which a customs agent looked through defendant's luggage, found a laptop, turned it on, clicked two innocuously-named icons,⁹⁸ and read the data they contained, all without suspicion that the defendant was carrying contraband of any kind.⁹⁹

In a reversal of the lower court's decision,¹⁰⁰ the Ninth Circuit

suspicion.”).

⁹⁵ *Id.* at 996-97.

⁹⁶ *Id.* at 997.

[T]he border search doctrine is not limited to those cases where the searching officers have reason to suspect the entrant may be carrying foreign contraband. Instead, “searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border.” *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). Thus, the routine border search of Romm's laptop was reasonable.

Id. (internal citations modified).

⁹⁷ *United States v. Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008) (“[W]e are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.”).

⁹⁸ *Arnold*, 533 F.3d at 1005. The icons were entitled “Kodak Pictures” and “Kodak Memories.” After examining the data, the officers determined the pictures contained child pornography. *Id.* (“When the computer had booted up, its desktop displayed numerous icons and folders. Two folders were entitled ‘Kodak Pictures’ and one was entitled ‘Kodak Memories.’ [The agents] clicked on the Kodak folders, opened the files, and viewed the photos on Arnold's computer including one that depicted two nude women.”).

⁹⁹ *Id.* at 1008.

¹⁰⁰ Judge Pregerson reasoned as follows:

The Court concludes that Fourth Amendment protection extends to the search of this type of personal and private information at the border. While not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive or other electronic storage device can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. This is because electronic storage devices function as an extension of our own memory. They are capable of storing our thoughts, ranging from the most whimsical to the most profound. Therefore, government intrusions into the mind—

found that searching the contents of a laptop computer was routine because it was analogous to the search of other containers such as briefcases, wallets, luggage, pictures, and films.¹⁰¹ Adopting the lopsided special needs balancing test,¹⁰² the Ninth Circuit rejected defendant's arguments that a laptop search is inherently highly intrusive because of a computer's immense capacity for data,¹⁰³ and rejected the argument that the search was performed in a "particularly offensive" manner.¹⁰⁴ As in *Flores-Montano*, *Ickes*, and *Romm*, the *Arnold* court determined the government had a nearly insurmountable interest from the outset, before considering individual privacy.¹⁰⁵

In the short time since its decision, *Arnold* has proven to be influential. Six days after the court announced its holding, U.S. Customs and Border Protection published its *Policy Regarding Border Search of Information (CBP Policy)*, echoing the constitutionality of suspicionless laptop searches at U.S. borders.¹⁰⁶ Since then, *Arnold* has been cited favorably,¹⁰⁷ and on February 23, 2009, the Supreme Court

specifically those that would cause fear or apprehension in a reasonable person—are no less deserving of Fourth Amendment scrutiny than intrusions that are physical in nature.

The Court further concludes that . . . any border search of the information stored on a person's electronic storage device [must] be based . . . on a reasonable suspicion. *United States v. Arnold*, 454 F. Supp. 2d 999, 1000-01 (C.D. Cal., 2006), *rev'd*, 533 F.3d 1003 (2008).

¹⁰¹ *Arnold*, 533 F.3d at 1007.

¹⁰² Citing *Flores-Montano*, the Ninth Circuit reasoned, "[t]he Supreme Court has stated that '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.'" *Id.* at 1008.

¹⁰³ *Id.* at 1008 ("[The defendant's] attempt to distinguish *Flores-Montano* is off the mark. The Supreme Court's analysis determining what protection to give a vehicle was not based on the unique characteristics of vehicles with respect to other property, but was based on the fact that a vehicle, as a piece of property, simply does not implicate the same 'dignity and privacy' concerns as 'highly intrusive searches of the person.'").

¹⁰⁴ *Id.* at 1009.

¹⁰⁵ *Id.* at 1006-08.

¹⁰⁶ See *supra* Part I (discussing the new *CBP Policy*).

¹⁰⁷ See *United States v. Singh*, No. 07-30421, 2008 WL 4426643 (9th Cir. Sept. 29, 2008) (holding unanimously that defendant's argument that a border search officer should have a reasonable suspicion to search defendant's laptop was foreclosed by *Arnold*); *United States v. Seljan*, 547 F.3d 993, 1011 (9th Cir. 2008) (Callahan, J., concurring) (decided on Oct. 23, 2008, citing *Arnold* for the proposition that the border search exception gives the government broad authority to search one's property as he enters the United States); *United States v. Hilliard*, No. 06-50709, slip op., 2008 WL 3850487, at *1 (9th Cir. Aug. 16, 2008) (denying the suppression of evidence found on hard drive during a routine border search); *United States v. Pickett*, No. 07-0374, 2008 WL 4330247 (E.D. La. 2008) (following *Arnold* and holding constitutional the border search of defendant's hard drive revealing evidence of child pornography after defendant crossed international waters and arrived at a port in Venice, Louisiana). But see *United States v. Cotterman*, No. 07-1207, 2009 WL 465028, at *3-5 (D. Ariz. Feb. 24, 2009) (granting defendant's motion for suppression of evidence found during a suspicionless non-routine extended border search of his computer, which occurred over the course of four days 170 miles from defendant's point of entry into the U.S. without a reasonable suspicion).

denied certiorari,¹⁰⁸ punting on its chance to correct the Ninth Circuit's holding. Therefore, lopsided, special needs reasonableness-balancing currently applies to even the most invasive searches of the data inside a traveler's laptop, leaving individual privacy unprotected. Yet this application is illogical because there is nothing special about the border when it comes to data. Therefore, the Court should not allow the government's interest to enter the balance with a predetermined advantage, and even-footing *Terry* analysis should apply.

II. THE GOVERNMENT'S INTEREST

Suspicionless border searches fail to satisfy the government's special need to secure the border¹⁰⁹ because there is no correlation between what crosses the border physically and what crosses via e-mail or internationally-accessible web-sites. Therefore, searching the data in one's computer at the border has little chance of preventing the entry of information or contraband via cyberspace. Further, customs agents should allocate their time in a way that maximizes border security. Performing time-consuming data searches without good reason prevents an agent from using her time to neutralize the risk that physically-harmful objects, such as weapons, explosives, poisons, and narcotics, will enter the border unchecked.

A. *Risk Analysis: The Government's Actual Interest in Searching Data at the Border*

There are a finite number of customs agents at the U.S. border and a nearly infinite number of potential threats,¹¹⁰ so it is the job of each agent to maximize border security by spending her time where the risk is greatest.¹¹¹ Therefore, where an agent's time is at a premium due to

¹⁰⁸ *Arnold*, 533 F.3d 1003, *cert. denied*, *Arnold v. United States*, No. 08-6708, 2009 WL 425169, at *1 (U.S. Feb. 23, 2009).

¹⁰⁹ See Paredes, *supra* note 29, at 15. Paredes proceeds from a similar premise, that "[t]he government's need to search the information crossing the border is attenuated by the intrinsic properties of a laptop's information. Ordinary containers present immediate threats to national security because of their capacity to carry physical objects." Further, "a laptop's information can carry . . . only informational contraband. By definition, information lacks the capacity to carry dangerous physical objects and thus cannot implicate the same governmental interest to search as an ordinary container." *Id.*

¹¹⁰ Statistics provided *infra*.

¹¹¹ CBP's mission statement reveals its central focus is to protect "the American homeland at and beyond our borders" from terrorism. The full mission statement is as follows:

We are the guardians of our nation's borders. We are America's frontline. We safeguard the American homeland at and beyond our borders. We protect the America

the number of travelers she must process, she should not focus on data. Because data travels via cyberspace, entirely circumventing the nation's physical borders, a customs agent is in a poor position to prevent its entry into the U.S. Instead, she should concentrate on preventing the entry of harmful *physical* items, which she is in the ideal position to stop.

To analyze why this is so, it is helpful to evaluate the different modes of travel for traditional containers—vehicles, suitcases, and the like—and for data. On an average day, CBP's 20,000 employees¹¹² process over one million passengers¹¹³ at the nation's 325 points of entry, including airports, seaports, and designated checkpoints at the Canadian and Mexican borders.¹¹⁴ CBP officers engage in searches targeting vessels that may contain contraband such as explosives, harmful weapons, drugs, monetary instruments, illegal aliens, and agricultural threats.¹¹⁵ The containers of these items take many forms, including a truck's dashboard, hollowed out shirt hangers, pellets of narcotics ingested into the body, and the freight areas of a barge.¹¹⁶ All

public against terrorists and the instruments of terror. We steadfastly enforce the laws of the United States while fostering our nation's economic security through lawful international trade and travel. We serve the American public with vigilance, integrity and professionalism.

U.S. CUSTOMS AND BORDER PROTECTION, SECURING AMERICA'S BORDERS AT PORTS OF ENTRY: OFFICE OF FIELD OPERATIONS STRATEGIC PLAN FY 2007–2011 4 (2006) [hereinafter STRATEGIC PLAN].

¹¹² *Id.* at 9.

¹¹³ *Id.* at 2. Specifically, the STRATEGIC PLAN states that more than 1.1 million passengers and pedestrians are processed at the borders each day. Of that number, 630,000 are aliens, 235,000 are air passengers, and 333,000 enter in privately owned vehicles. Additionally, CBP is responsible for inspecting 79,000 shipments of goods. This amounts to an "annual flow of over 400 million people." *Id.*

¹¹⁴ *Id.* at 9–11. Annually, CBP clears over 80 million air passengers and crew according to statistics from 2005. *Id.* at 9. At land border crossings, over 319 million passengers and pedestrians were processed in 2005. *Id.* at 11. Typically, each passenger must provide identification, and is subject to "further inspection." *Id.* At seaports, the major focus is cargo processing. In 2005 CBP processed more than 26 million passengers and crew and 11 million cargo containers. *Id.* at 12. The search procedures vary depending on the kind of port and its geographic location, and CBP attempts to create flexible policies to counter potential threats with "unpredictability." *Id.* at 11.

¹¹⁵ *See id.* at 15–16.

¹¹⁶ A survey of CBP's press releases for the month of December 2008 lends support to the idea that invasive border searches may be an essential means of preventing the entry of contraband inside traditional containers. *See* CBP Newsroom, *Border Patrol Seizes More Than 2 Tons of Marijuana Near Tucson Over Weekend*, Dec. 1, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12012008.xml (seizure of 1,100 pounds of marijuana inside a vehicle at Arizona's border with Mexico); CBP Newsroom, *CBP, Coast Guard Team Up to Intercept Stowaways*, Dec. 2, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12022008_4.xml (seizure of three stowaways aboard a barge off Mobile, AL); CBP Newsroom, *Laredo Border Patrol Agents Seize More Than a Ton of Marijuana*, Dec. 4, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12042008_2.xml (seizure of 2,572 pounds of marijuana inside a tractor trailer, uncovered by

such items and their containers, unlike data, share the element of tangibility. To get these items into the country, a criminal would have to drive, carry, or mail them through the country's physical borders. Therefore, the only way to keep these items out is to search traditional containers *at the border*.

Data, on the other hand,¹¹⁷ may readily enter the U.S. within seconds from anywhere in the world without stopping at a physical border.¹¹⁸ Data is intangible; it can be copied easily and moved quickly from one computer to another.¹¹⁹ One can send data into the country

gamma rays revealing an irregularity in the rear portion of the truck at the Laredo, TX border); CBP Newsroom, *CBP's Sharp Skills Stop Dope Filled Pencil Sharpener*, Dec. 8, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12082008_4.xml (seizure of 8.6 ounces of opium inside a pencil sharpener, discovered at an air cargo facility in Memphis, TN); CBP Newsroom, *CBP in Atlanta Discovers Cocaine Concealed in Wooden Hangers*, Dec. 9, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12092008.xml (seizure of cocaine, hidden in wooden hangers packed in a suitcase at Atlanta Hartsfield-Jackson International Airport); CBP Newsroom, *Brownsville CBP Seizes 29 Heroin-Filled Pellets from Carrier's Digestive Tract*, Dec. 9, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12092008_4.xml (seizure of 381 grams of heroin, smuggled internally by a male at the Brownsville, TX port of entry); CBP Newsroom, *CBP Officers at Calexico Downtown Port of Entry Foil Cocaine Smuggling Attempt*, Dec. 11, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12112008.xml (seizure of thirty-nine pounds of cocaine, concealed in a specially built compartment in a truck bed at the Calexico downtown port of entry); CBP Newsroom, *CBP Officers at Newark Airport Seize More Than 12 Pounds of Cocaine, Make 2 Arrests*, Dec. 12, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12122008_4.xml (seizure of more than twelve pounds of cocaine, concealed in two false-sided suitcases at Newark airport); CBP Newsroom, *4,971 Pills of Ecstasy Seized at Ambassador Bridge*, Dec. 15, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12152008.xml (seizure of 4,971 pills of ecstasy, hidden in the rear wheel well of a car and discovered with a gamma ray device at Ambassador Bridge); CBP Newsroom, *El Paso CBP Seizes Steroids Hidden in Dashboard, Marijuana from Tractor-Trailer*, Dec. 15, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12152008_8.xml (seizure of 150 vials of anabolic steroids, hidden in the dashboard of a car at Paso Del Norte international crossing from Mexico); CBP Newsroom, *CBP Seizes More Than 11 Pounds of Marijuana Hidden in African Artwork*, Dec. 16, 2008, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/december_2008/12162008_6.xml (seizure of eleven pounds of marijuana, hidden in African artwork and discovered via the X-ray examination of international air cargo at the Philadelphia airport).

¹¹⁷ A close inspection of Internet traffic statistics suggests rates of international file migration vastly outnumber passenger travel. See Internet World Stats, Internet Usage Statistics: The Internet Big Picture, <http://www.internetworldstats.com/stats.htm> (using Internet usage statistics for March 31, 2009, based on population statistics collected by the U.S. Census Bureau and internet usage information from Nielsen/NetRatings) (last visited Aug. 20, 2009).

¹¹⁸ In 2009, 23.8% of the world's population, or 1,596,270,108 people, were connected to the Internet. Of those users, 15.7% were inside the U.S., leaving 84.3% of the world's Internet-using population outside the nation's borders. For example, Asia accounts for 41.2% and Europe accounts for 24.6% of the world's Internet-using population. *Id.*

¹¹⁹ From almost anywhere in Asia, Europe, South America, and Australia, an Internet user can send a file into the U.S. in less than one-fifth of a second. See Internet Traffic Report, <http://www.internettrafficreport.com/> (last visited Aug. 20, 2009). This website provides Internet efficiency updates every five minutes, reporting how fast a file can be sent or "pinged" around the

from a foreign computer via e-mail or post it to a website accessible worldwide. Intercepting harmful data—such as evidence of a terrorist plot, child pornography, or financial records of illegal activity—at the nation’s border does little to prevent its entry into the U.S. because of the unusual way data travels.¹²⁰ Moreover, given the large number of passengers crossing the border¹²¹ relative to the low number of CBP agents,¹²² it is incredibly inefficient to perform lengthy data searches at the border to promote security.¹²³ Therefore, in contrast to searching

globe through an international series of web servers. *See id.* at Frequently Asked Questions, <http://www.internettrafficreport.com/faq.htm#about> (last visited Aug. 20, 2009). In this respect, the statistics on the site function almost like an Internet weather report where good weather equates to high-speed file transfer and bad weather equates to a slower speed. On Aug. 20, 2009, the weather was good everywhere. The average ping speed across Asia, North and South America, Europe, and Australia was about 200 ms, or one-fifth of a second. The website also reflects the integrity of the files upon return to their origin, and is measured by the concept known as “packet loss.” *Id.* Essentially, a file is broken down into discrete packets before it is sent over the Internet. If a user sends twenty and only nineteen return, the packet loss is 5%. A packet loss of this magnitude is relatively undetectable to the user. *Id.* On Aug. 20, 2009 average packet loss across major Internet servers was less than 2%, under the detectable threshold. This means on Aug. 20, 2009 the average Internet user could send a file around the world from almost anywhere in the world in about a fifth of a second.

¹²⁰ Data travel is unusual because of the speed and magnitude with which it can travel as compared to traditional containers, which are sent into the U.S. with people or in mail or cargo containers. Using Chicago’s Internet traffic as a national exemplar, recently-gathered statistics demonstrate the volume of incoming information through Chicago’s Internet servers measured in kilobytes per second. *See* Gloriad, Global Ring Network for Advanced Applications Development, <http://www.gloriad.org> (last visited Aug. 20, 2009) (search “average bps month” for updated statistics representing the rates at which Russia, China, and Korea send electronic information into the United States). A kilobyte is roughly one half page of text in a word processor. *See* WiseGeek.com, How Much Text is in a Kilobyte or Megabyte?, <http://www.wisegeek.com/how-much-text-is-in-a-kilobyte-or-megabyte.htm> (last visited Aug. 20, 2009). From July 21, 2009 through Aug. 20, 2009, the average amount of digital information flowing into Chicago from Russia was about 135,000,000 kilobytes per second or about 67,500,000 pages of text per second. *See* Gloriad, *supra*. For the same period of time, China sent well over 5,000,000,000 kilobytes per second, *see id.*—or the equivalent of 5,000,000 thick books, *see* WiseGeek.com, *supra*—into Chicago. Korea sent about 70,000,000 kilobytes per second. *See* Gloriad, *supra*.

¹²¹ In 2007, for example, Chicago received 1,140,000 international visitors. *See* CHICAGO OFFICE OF TOURISM, 2007 STATISTICAL INFORMATION 2 (2007), available at http://www.explorechicago.org/etc/medialib/explore_chicago/tourism/pdfs_press_releases/chicago_office_of.Par.83640.File.dat/Statistics2006050708FINAL.pdf (or search “Google” for “Chicago Office of Tourism Statistics” then follow “Chicago Office of Tourism” link to automatically download the pdf). Divided over twelve months, this statistic suggests over two international passengers per minute arriving into Chicago.

¹²² *See supra* notes 112-114 and accompanying text.

¹²³ Given the huge volume of travelers processed by CBP, its touchstone of success is efficiency. An executive summary suggests CBP’s goal is to “conduct the right level of inspection, based on well-developed risk assessment methods.” *See* STRATEGIC PLAN, *supra* note 111. CBP’s executive summary states the following:

To protect America from harm, CBP must detect and remove the people and goods that pose a threat from the legitimate annual flow of over 400 million people, 20 million cargo containers, and 130 million conveyances. Given this enormous volume . . . CBP must set and conduct the *right level of inspection*, based on well-developed risk assessment methods, while recognizing the vast majority of people and goods are

traditional containers,¹²⁴ suspicionless border searches of the data inside laptops are unlikely to protect the border.

A simplified hypothetical illustrates the argument. Suppose a terrorist organization wants to detonate bombs in a U.S. city, and the organization has some operatives inside the city and others in a foreign country. Suppose also that its operatives inside and outside the U.S. both have access to explosives. To achieve its criminal goals, the organization uses several methods to increase the likelihood of detonation. First, the organization sends two operatives on two different planes to smuggle bombs into the U.S. city. The first operative puts the bomb in a suitcase and the second converts his laptop into a bomb. To further increase the chances of achieving its goals, the organization develops a backup plan, directing its operatives already inside the U.S. city to detonate explosives already hidden inside the city. The organization distributes the plan in two ways. First, it sends an operative on a plane with a laptop (not the bomb-bearing laptop mentioned *supra*) containing an encrypted file outlining the plan. Second, it sends the same information in a coded e-mail to all its operatives inside the U.S. city.

The only way to thwart the entry of either bomb—those hidden in the passengers' traditional containers—would be to search and seize the containers themselves. Detecting the bombs during a border search would be the only way to keep them out of the country. Each instance of detection would, itself, protect the U.S. from a harmful explosion. As for the bomb disguised as a computer, there would be absolutely no need to search the data inside the computer to determine if the computer, itself, was a bomb. Simply looking inside the computer—or even asking the passenger to turn it on—would effectively determine if the computer, *itself*, posed a threat to the nation's security.

With respect to the detonation plans, the analysis reaches the opposite result. Even a successful seizure of the plans contained in the encrypted data inside the laptop—which would be a remarkably fortuitous result given the suspicionless nature of the search—would have no bearing on the data sent by e-mail.¹²⁵ In this way, data is distinguished from traditional containers because stopping data at the

legitimate. These inspections must uncover violations, and accurate determinations must be made from the results.

Id. (emphasis added).

¹²⁴ Alzhabi, *supra* note 26, at 181 (“One can think of a laptop as a closed container, which, as a general matter, may be searched during a routine border search.”).

¹²⁵ The purpose of this argument is *not* to suggest that the government should monitor all e-mails at all times flowing into the U.S. from foreign countries. Rather, the point is that such searches are already in place. The specifics of these e-mail searches are the focus of note 143. Determining what methods are most appropriate to detect breaches in security transferred over e-mail is a topic outside the scope of this Note; however, it is clear that the executive branch has used FISA (Foreign Intelligence Surveillance Act) as a tool to monitor harmful data. *Id.*

border has no bearing on whether it will enter the country electronically. The physical border is entirely insignificant in the analysis, so the logic of the border search exception completely misses the mark with respect to data.

Critics counter that the detection of even one copy of the detonation plans would help thwart a terrorist plot and increase the nation's security.¹²⁶ On its face and in a vacuum, if CBP were to have unlimited resources to instantly and successfully identify harmful data, this argument would be persuasive. In reality, however, CBP consists of a limited number of officers with a limited amount of time for each search.¹²⁷ Practical and logistical limitations¹²⁸ require officers in the field to make prospective moment-to-moment determinations based on their experience, which tells them where risk is most likely to exist.¹²⁹ Surely, it cannot be the best use of an officer's time to perform a lengthy laptop search on a mere whim, without any suspicion of risk whatsoever.¹³⁰ Additionally, even if CBP spends the time to locate an encrypted e-mail, it is still possible that an e-mail with the same content has already traveled to operatives in the U.S. So, by the time CBP decrypts and acts, it will be too late to prevent harm. Further, the counterargument proves too much, since the fact the data was found *at the border* is irrelevant. That is, the counterargument is equally a justification for suspicionless searches *anywhere*, which cannot be the

¹²⁶ See Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1097-98 (2009) (“[T]he fact that terrorists and others might use a number of techniques to commit their crimes does not diminish the magnitude of the government’s interest in inhibiting [a] particular technique.”).

¹²⁷ See *supra* notes 111-114 and accompanying text (suggesting the number of travelers CBP processes is overwhelming in comparison to the number of CBP employees performing the searches).

¹²⁸ *Id.*

¹²⁹ To maximize its ability to protect the U.S., CBP seeks to efficiently allocate its valuable time and resources to where the risk of harm is greatest. See STRATEGIC PLAN, *supra* note 111 at 10 (“The examination level of international cargo within the air environment depends on the risk assigned and availability of facilities and resources.”); see also *id.* at 17 (“The use of advanced technology and human capital to analyze data, model scenarios, and align actions with assessed risk levels is central to CBP’s proactive approach to operations.”); *id.* at 30 (discussing its method of analyzing risk in an effort to maximize CBP’s effectiveness at POE’s [Points of Entry]: “Inspection efficiency directly affects CBP mission delivery, as shorter processing times for low-risk people and goods translate into more time to focus on higher risks. Continued success at POEs requires CBP to . . . [verify] that all people and goods are *inspected appropriately*.”) (emphasis added); *id.* at 31 (“Lower-risk travelers and shipments should undergo a less in-depth inspection than those of higher-risk. While the depth of examinations involves the use of defined risk management principles, the inspection of people or goods must also include the discretion of the CBP officer.”).

¹³⁰ Indeed, where a CBP agent can articulate one reason why she feels searching a laptop’s data is necessary to pursue the nation’s security, she should be given the leeway to make the appropriate search. The purpose of this Note is merely to require agents to have some articulable reason to dedicate valuable time and resources to the lengthy process of mining the data inside one’s computer. Unfortunately, the current *CBP Policy* requires no level of suspicion whatsoever. See *CBP Policy*, *supra* note 2, § (B).

right result.¹³¹ Finally, suspicionless searches could just be a cover for profiling¹³² or other illegitimate motivations to search, such as harassing a difficult traveler.¹³³ Therefore, the *suspicionless* component is the problem with the *CBP Policy*.

In the above hypothetical, for example, to discover the detonation plans in the encrypted data inside the laptop, a CBP agent would have to spend quite a bit of time on her search,¹³⁴ compromising the thoroughness with which she could search all the other passengers on the plane. The computer search would entail turning on the computer, searching the hard-drive, sending it for decryption, and waiting for a report. Were she to spend all her time on the suspicionless laptop search of a low-risk passenger, the search would constitute a clear breach of department policy, which requires the proper allocation of its officers' time and resources.¹³⁵ From this perspective suspicionless data searches actually jeopardize the government's special need to protect the border.¹³⁶

Doctrinally, this analysis is significant for two reasons. First, it illustrates why the justifications for the special needs doctrine are

¹³¹ For a more in depth discussion of this illogical outcome, see notes 139-142 and accompanying text.

¹³² While it is true that the Supreme Court has not specifically held that searches based on racial profiling are automatically unconstitutional, the Court's language has hinted at its view that profiling without more is not a valid reason to stop and search someone. *Atwater v. City of Lago Vista*, 532 U.S. 318, 372 (2001) (O'Connor, J., dissenting) ("Such unbounded discretion carries with it grave potential for abuse. . . . Indeed, as the recent debate over racial profiling demonstrates all too clearly, a relatively minor traffic infraction may often serve as an excuse for stopping and harassing an individual."); see also *Illinois v. Wardlow*, 528 U.S. 119, 132-35 (2000) (Stevens, J., dissenting). In this 5-4 decision, Justice Stevens took judicial notice that the problem of racial profiling is "real—not imagined." *Id.* at 133 n.10 (citing studies demonstrating the pervasiveness of the racial profiling of minority individuals).

¹³³ Attorneys who state loudly that they "know their rights" come to mind.

¹³⁴ According to the *CBP Policy* itself, decryption may be so complicated that the laptop could be shipped off-site. See *CBP Policy*, *supra* note 2, § (C)(1). The time and resources entailed in this process would further tie up valuable CBP resources, all on the whim of an officer who chose to search a computer's data. Of course, where the officer chose to perform the data search on something *more* than a mere whim, the search would not be suspicionless, and the concerns of this note would not apply.

¹³⁵ See STRATEGIC PLAN, *supra* note 111, at 10, 17, 23, 28, 30-31, 33, 43, 46 (demonstrating that promoting accurate "risk" analysis is CBP's central goal upon which nearly all of its methods and processes are based).

¹³⁶ The facts of a recent case in the District of Arizona provide one fitting example of the misallocation of resources encouraged by the *CBP Policy*. *United States v. Cotterman*, No. 07-1207, 2009 WL 465028 (D. Ariz. Feb. 24, 2009). Based on a criminal conviction for child sex crimes fifteen years in the past, which "clear[ly]" did not give rise to a reasonable suspicion, border officers detained the defendant and his wife for eight hours, combing through all of their belongings. *Id.* at *7, *1-2. Despite not finding any contraband, one agent seized the couple's computers, searched them for four days, then drove them 170 miles to a computer expert who mined the computer's hard drive, eventually finding child pornography. *Id.* at *3. Despite the fortuitous discovery of illegal images, it can hardly be argued that tying up numerous officers for the better part of a week is the best way to prevent the types of activity—namely terrorism—that the *CBP Policy* was designed to prevent.

inapplicable to data. Second, it demonstrates why the government's and the individual's interests should enter the balance on even footing since the government's need to search data is not special.

B. *The Border Search and Special Needs Doctrines Do Not Apply to Data*

The government has the same need to search data at the border as it does to search data inside computers already in the U.S.¹³⁷ Consequently, this need is not "special" under Supreme Court doctrine,¹³⁸ so the special needs doctrine should not apply. In the context of searching a laptop's data, the doctrine would require the existence of something special about searching the data *at* the physical border relative to searching data in computers already inside the country. As demonstrated in the previous section's hypothetical, this simply is not the case. Further, since data found at the border has no special ability to enter the country, and an individual's privacy interest in her data is generally the same at the border and inside the country,¹³⁹ it is illogical to require a suspicion in one place and not the other. Therefore, a suspicion requirement should exist in either both places or neither place.

The latter option would convert every computer *already inside the U.S.* into an international border, subjecting homes, offices, and bedrooms¹⁴⁰ to government searches based on a mere whim. This absurd conclusion would effectively eliminate the Fourth Amendment altogether. Mountains of authority suggest the government does not have such unfettered access to one's home.¹⁴¹ Additionally, emerging

¹³⁷ Erwin Chemerinsky, *Laptop Search at Border Was Illegal*, L.A. DAILY JOURNAL, Nov. 29, 2006, at 6. Professor Chemerinsky argues that the special needs doctrine, upon which the courts have justified border searches, only applies where there is something special about the border. For computers, there is nothing special about the nation's physical borders:

The government has no special interest at the border in searching a person's computer different from computers that are already in the country. The government is allowed to engage in suspicionless border searches where there is an interest unique to the border, such as preventing people from entering illegally or in intercepting drugs or weapons being brought into the country. But these interests do not exist with regard to the memory of computers.

Id.; see also Paredes, *supra* note 29, at 15.

¹³⁸ See *supra* Part II.A.

¹³⁹ An individual's privacy interests in the data inside her laptop are the focus of Part III.

¹⁴⁰ One's privacy in her home is the central protection of the Fourth Amendment, dating back to the Framers' explicit intent. *Segura v. U.S.*, 468 U.S. 796, 810 (1984) ("The sanctity of the home is not to be disputed. . . . [T]he home is sacred in Fourth Amendment terms . . . because of [one's] privacy interests in the activities that take place within."); *Berger v. State of N.Y.*, 388 U.S. 41, 50 (1967) (citing *Boyd v. U.S.*, 116 U.S. 616, 627 (1886)).

¹⁴¹ See, e.g., DRESSLER & THOMAS, *supra* note 14, at 205. Collecting cases in support of the following proposition, and delineating narrow exceptions to it, Professor Dressler explains, "the

scholarship and case law suggests electronic communications such as e-mails and website content are protected by some level of suspicion under the *Foreign Intelligence Surveillance Act* (FISA).¹⁴²

Therefore, the former option, requiring some level of suspicion before searching data at the border, makes much more sense. Data searches based on a suspicion would protect individual privacy by prohibiting invasive data searches unless there was “one good reason” to perform the search. Additionally, this requirement would encourage officers to focus their efforts on detecting harmful data where the risk of that harm is greatest. Finally, a suspicion requirement at the border would comport with similar, existing requirements for searching data inside home computers and data sent via cyberspace.

One may argue that requiring some suspicion for all data searches—those performed at the border and those performed under FISA¹⁴³ in the nation’s interior—gives criminals a free pass to transfer

Supreme Court has hesitated to give the police a free rein to enter a home without a warrant.” *Id.*; *see also* *Welsh v. Wisconsin*, 466 U.S. 740 (1984):

It is axiomatic that the “physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.” And a principal protection against unnecessary intrusions into private dwellings is the warrant requirement imposed by the Fourth Amendment on agents of the government who seek to enter the home for purposes of search or arrest. It is not surprising, therefore, that the Court has recognized, as “a ‘basic principle of Fourth Amendment law[,]’ that searches and seizures inside a home without a warrant are presumptively unreasonable.”

Id. at 748-49 (internal citations demonstrating weight of authority omitted).

¹⁴² Generally, FISA, discussed in greater detail at note 143, requires some level of suspicion to search electronic communications. LAFAVE, *supra* note 17, § 4.9(b) (discussing the Foreign Intelligence Surveillance Act). An in-depth discussion of the government’s ability to search e-mails and websites connected to computers already inside the U.S. is outside the scope of this Note, which argues officers must have a one good reason to search the data inside one’s laptop at the nation’s physical borders. However, the following brief discussion demonstrates searches of the data inside one’s computer located *inside* the country requires some level of suspicion.

¹⁴³ Generally, “FISA requires the executive branch to apply for and obtain court orders to conduct foreign intelligence surveillance from the Foreign Intelligence Surveillance Court,” and “if the government seeks evidence of domestic security violations, it must follow the usual criminal law authorities.” LAFAVE, *supra* note 17, § 4.9(b). Under 50 U.S.C.A. § 1801(f) (West 2008), FISA regulates the government’s ability to engage in “electronic” surveillance. *Id.* Essentially, “the government needs a FISA court order to intercept the contents of known United States persons inside the United States . . . [and] to collect communications sent over a wire if the interception occurs inside the United States.” *Id.* Alternatively “[n]o court order is required if surveillance is ‘directed at a person reasonably believed to be located outside the United States.’” *Id.* A pen register (capturing the address and subject lines of an e-mail, as opposed to the e-mail’s content itself), “if investigators submit a certification that the information likely to be obtained . . . ‘is relevant to . . . protect against international terrorism or clandestine intelligence activities.’” *Id.* Additionally, “[t]he records sought must be ‘relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.’” *Id.* Finally, the scope of the government’s authority to reproduce, inspect, or alter material in which a person has a reasonable expectation of privacy with respect to the contents of communications with ISPs (Internet Service Providers), is unclear. *Id.* Generally, however, 50 U.S.C.A §§ 1821-29 require the government to establish probable cause that:

(A) The target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power

data. In turn, this incentivizes criminal conduct over e-mail and the Internet, while at the same time tying an officer's hands to combat it. But this argument falsely assumes that requiring *any* level of suspicion decreases an officer's effectiveness in ferreting out and preventing crime. Surely it does not. Rather, it encourages an officer to pursue searches based on risk assessment that the officer's training and experience reinforce.¹⁴⁴

Since the government has no special need to search the data inside a traveler's computer at the border, the government's interest should not be elevated automatically before entering the Fourth Amendment's reasonableness-balancing test. Instead, as in *Terry*, the government's and individual's interests should enter the balance on even footing, and the government's interest in performing a data search should only prevail when a customs agent has one good reason to believe the traveler's data contains criminal information. Where no good reason exists, the Court should find the individual's privacy interests superior.

III. THE INDIVIDUAL'S PRIVACY INTEREST IN HER LAPTOP'S DATA

A. Existing Privacy Rationales

Scholars have focused numerous persuasive arguments¹⁴⁵ on the heightened privacy interest in the data inside a laptop.¹⁴⁶ First, travelers have made several arguments against the *CBP Policy*.¹⁴⁷ Muslim, Arab, and South-Asian travelers argue that the *Policy* is a ruse for unconstitutional racial, ethnic, and religious profiling.¹⁴⁸ Business

solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and (B) the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power[.]

Id. (citing 50 U.S.C.A. § 1824(a)(3) (West 2008)).

¹⁴⁴ See STRATEGIC PLAN, *supra* note 111.

¹⁴⁵ In his comprehensive recent article arguing against the Ninth Circuit's holding in *Arnold*, Paredes addresses a number of individual data privacy arguments. Paredes, *supra* note 29, at 16-22; see also Sales, *supra* note 126, at 1100-01 (summarizing these scholarly arguments).

¹⁴⁶ For the purposes of this discussion, the term "laptop" incorporates by analogy cell phones, memory drives, iPods, PalmPilots and the like, all of which are searchable under the *CBP Policy*.

¹⁴⁷ *Hearings*, *supra* note 5. At the Senate hearings various advocacy groups voiced their opinions on the (then) unpublished customs policy of performing suspicionless data and laptop searches. *Id.* Those groups, including the Association of Corporate Travel Executives, the Electronic Frontier Foundation, and Muslim Advocates, addressed the public's reproach for the *CBP Policy*. *Id.* Generally, the testimony of these advocacy groups reflected the sentiment that laptop searches represent an unwarranted invasion of one's privacy. *Id.* Supporters of the *CBP Policy* argued the searches were necessary to ensure the safety of the nation's borders. *Id.* The specific arguments on both sides of the issue are discussed in greater detail *infra*.

¹⁴⁸ See *Hearings*, *supra* note 5 (testimony of Farhana Khera, President and Executive Director of Muslim Advocates). Ms. Khera's testimony includes two examples of CBP's search and

travelers argue suspicionless data searches jeopardize profitable relationships when clients find out the government has seen privileged documents.¹⁴⁹ Technological experts argue evidence collection technology threatens to make invasive laptop searches standard at the border, compounding the government's invasion of personal privacy.¹⁵⁰ Scholars and advocates have also argued data searches violate the First Amendment, which protects content.¹⁵¹

Additionally, some have argued that the computer's vast capacity for data makes it similar to the human mind.¹⁵² In *Arnold*, the Ninth Circuit explicitly rejected this argument;¹⁵³ however, emerging medical technology will make this link between the human body and computers more difficult to reject in the future.

interrogation of Muslim Americans. One traveler—an executive vice president at a major technological firm in Seattle, a husband, father of three, and a community and business leader—complained of being searched on eight separate occasions where CBP agents copied his documents, seized his cell phone, and interrogated his family about the mosque they attend. *Id.* Another traveler—a Pakistani corporate lawyer, who graduated from top U.S. schools—complained of twenty or more occasions where CBP agents “lost” her bags, pulled her aside, searched her digital camera, viewed images of her mother, friends, and family, asked her to identify them, and asked her whom she supports in the upcoming Presidential election. *Id.* Similarly, Jawad Khaki, a fifty-year-old corporate executive who had been a U.S. citizen for twenty-three years, told *U.S.A Today* that each time he travels into the U.S., border patrol agents force him to turn over his smart phone, provide the password, and answer questions regarding his contacts and calendar. See Gannett News Service, *Electronics Subject to Search at Border*, U.S.A. TODAY, July 7, 2008, available at http://www.usatoday.com/tech/news/techpolicy/2008-07-06-laptopsearch_N.htm?loc=interstitialskip.

¹⁴⁹ See *Hearings*, *supra* note 5 (testimony of Susan Gurley); see also Odean L. Volker, *Lawyers, Laptops, and the Border*, 72 TEX. B.J. 640, 640-42 (2009) (arguing that laptop searches at the border force business travelers to choose between losing work time by leaving their laptops at home or travelling with their work computers and risking a breach of client confidentiality).

¹⁵⁰ See *id.* (testimony of Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation). Specifically, Mr. Tien mentions Microsoft COFEE, a USB thumb-drive that can efficiently mine electronic information found on a laptop, and the CSI Stick, capable of quickly capturing the data on most cell phone models. *Id.*

¹⁵¹ Brief for Association of Corporate Travel Executives and Electronic Frontier Foundation as Amici Curiae Supporting Defendant-Appellee at 22, *United States v. Arnold*, 533 F.3d 1003 (2008) (No. 05-772) [hereinafter *Amici Brief*], available at http://www.eff.org/files/filenode/US_v_arnold/arnold_amicus.pdf. See also Paredes, *supra* note 29, at 21 (“Although one’s First Amendment rights may be attenuated at the border claims made at the border [sic], the interest in protecting the free flow of ideas must be added to . . . individual interests.”).

¹⁵² *Amici Brief*, *supra* note 151, at 11-16.

¹⁵³ *Arnold* 533 F.3d at 1007-08 (“[A] piece of property . . . simply does not implicate the same ‘dignity and privacy’ concerns as ‘highly intrusive searches of the person.’”) (internal citation omitted).

B. “Person-Dignity” in *Arnold and Flores-Montano*¹⁵⁴

To frame this discussion, it is helpful to look at defendant’s arguments in *United States v. Arnold*,¹⁵⁵ and how the Ninth Circuit drew on *Flores-Montano* to reject the arguments. The defendant in *Arnold* argued that suspicionless laptop searches are highly invasive and particularly offensive because their capacity approximates that of the human mind.¹⁵⁶ Therefore, an officer should have some level of suspicion before searching its data.¹⁵⁷ The court flatly rejected these arguments, citing *Flores-Montano* for the proposition that at the border, the government’s interest controls.¹⁵⁸

In *Flores-Montano* the Court evaluated a border search involving property.¹⁵⁹ The Court created a bright line between the search of property and the search of the human body. Specifically, the Court held that a property search was routine, requiring no level of suspicion, whereas a search of the human body might be non-routine, requiring some level of suspicion.¹⁶⁰ The Court’s test for drawing this bright line was where a search would invade one’s “person-dignity.”¹⁶¹ The Court has included in this category “strip, body-cavity, or involuntary x-ray searches.”¹⁶² Therefore, the bright line begins and ends at the skin.

The Ninth Circuit applied this bright line rule, holding that searching a computer, whether or not its capacity for data made it like the human mind, did not literally constitute getting inside a person’s skin.¹⁶³ Therefore, it held that suspicionless data searches are routine,

¹⁵⁴ *Id.* at 1007 (citing *Flores-Montano*, 541 U.S. at 152, in turn citing *Montoya de Hernandez*, 473 U.S. at 541).

¹⁵⁵ 533 F.3d 1003.

¹⁵⁶ *Id.* at 1006.

¹⁵⁷ *Id.*

¹⁵⁸ *Id.* at 1007 (“In other words, the ‘Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.’”) (quoting *Flores-Montano*, 541 U.S. at 152).

¹⁵⁹ *Flores-Montano*, 541 U.S. at 150 (finding that the property in question was the gas tank of defendant’s car).

¹⁶⁰ *Id.* at 152 (“[T]he 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.”). In an earlier border search opinion involving cocaine-filled balloons in a woman’s alimentary canal, the Court explicitly withheld judgment on what level of suspicion would be required for a nonroutine search to be reasonable. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 n.4 (1985) (“Because the issues are not presented today we suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches.”).

¹⁶¹ *Flores-Montano*, 541 U.S. at 152.

¹⁶² *Montoya de Hernandez*, 473 U.S. at 541 n.4.

¹⁶³ *Arnold*, 533 F.3d at 1007-08.

reasonable, and do not violate the Fourth Amendment.¹⁶⁴ However, emerging medical technology, which actually allows its user to monitor the inside of his body on a computer screen, provides the seeds for the rejecting the Ninth Circuit's holding in *Arnold*.

C. *A New Privacy Rationale: The Increasing Body-Computer Nexus*

The Association of Corporate Travel Executives and the Electronic Frontier Foundation submitted briefs in support of the defendant in *Arnold*, arguing that laptop searches are “uniquely invasive.”¹⁶⁵ They relied on an influential article by Professor Kerr observing that technology has the potential to close the gap between a person and her computer. Specifically, Kerr argues that the growing memory capacities of computers allow them to hold large “chunk[s] of our lives.”¹⁶⁶ In turn, they become increasingly private. In addition to a computer's increasing capacity for data,¹⁶⁷ computer programming has the ability to make one's computer a highly customized and personalized fixture in one's life.¹⁶⁸ Today, a computer can predict its user's musical taste¹⁶⁹ or sexual compatibility,¹⁷⁰ functions associated with the human mind. More startlingly, however, is the computer's

¹⁶⁴ *Id.*

¹⁶⁵ *Amici Brief*, *supra* note 151, at 15.

¹⁶⁶ Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005):

As our computers perform more functions and preserve more data, we may eventually approach a world in which a considerable chunk of our lives is recorded and stored in perpetuity in our computers. These details may end up stored inside our machines in a way that can be reconstructed later by a forensic analyst with remarkable accuracy.

Kerr also discusses a computer's ability to record its user's Internet history, further demonstrating how a suspicionless search of a computer's data is uniquely invasive:

[B]rowsers used to surf the World Wide Web can store a great deal of detailed information about the user's interests, habits, identity, and online whereabouts, often unbeknownst to the user. Browsers typically are programmed to automatically retain information about the websites users have visited in recent weeks; users may use this history to retrace their steps or find web-pages they previously visited.

Id. at 543.

¹⁶⁷ When Kerr published his article in 2005, computers had an average capacity of eighty gigabytes, roughly the amount of information contained in one floor of an academic library. *Id.* at 542. In 2008, Apple's entry laptop model comes in options ranging from one hundred sixty gigabytes to two hundred fifty gigabytes of hard-drive space, roughly three times the capacity of the computers with which Kerr was concerned. *See* Apple.Com, Apple Store, <http://store.apple.com/us> (last visited July 26, 2009).

¹⁶⁸ Kerr, *supra* note 166, at 569 (“[C]omputers are playing an ever greater role in daily life and are recording a growing proportion of it. In the 1980s, computers were used primarily as glorified typewriters. Today they are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.”).

¹⁶⁹ iPod's recently released “Genius” function analyzes the songs in one's computer and makes predictions about what music the person will enjoy.

¹⁷⁰ Numerous websites such as eharmony.com, match.com, and jdate.com predict romantic compatibility by analyzing one's personal profile.

increasing ability to monitor the inside of one's body, essentially breaching the skin, creating an intimate nexus between the computer and the body.

Certain medical programs—some already in existence and some in development—are actually beginning to monitor what is beneath the human skin and project it to the screen of a laptop.¹⁷¹ New diabetes and heart monitors include small devices implanted *beneath* the skin that relay insulin and blood pressure data to the laptop's screen. A host of other programs are available for the iPod, allowing doctors and other users to monitor the interior of the body.¹⁷² While some of the data can only be interpreted by medical professionals, the focus of some computer applications is to make them so readily understandable that

¹⁷¹ In existence and in development are several programs and computer functions that are undeniably linked to the biomedical processes of the human body and the neurological functions performed by the brain. Essentially, these programs relay information from inside one's body to his computer. Therefore, by searching one's computer it is increasingly possible literally to look *inside* one's body at his insulin levels, heart rate, and thought processes. For example, Adaptive Path is a company that specializes in generating technological solutions for medical problems. See Adaptive Path, About Us, <http://www.adaptivepath.com/aboutus/> (last visited July 28, 2009) (setting forth the company's mission, "to deliver great experiences that improve people's lives, while sharing our advances in the field with our clients, partners, and peers."). Recently, the company has been developing a device called the Charmr, intended to streamline a Type 1 Diabetic's ability to monitor her insulin levels. See Adaptive Path Charmr Page <http://www.adaptivepath.com/blog/category/charm-project/> (describing the device as combining a "glucose pump and a monitor for Type 1 Diabetics") (last visited July 28, 2009). The design contains three pieces. The first piece is an insulin pump attached to a needle to be inserted beneath one's skin. This device wirelessly relays information from beneath the user's skin to the Charmr, the second piece. The Charmr itself is a small wirelessly-enabled thumb drive that can be tucked in one's pocket or worn around the neck. See DARREN MURPH, CHARMR CONCEPT TRANSFORMS GLUCOSE MONITORING (2007), <http://www.engadget.com/2007/08/15/charm-concept-transforms-glucose-monitoring/>. When the Charmr is completed, it will continuously monitor glucose levels and store data for future analysis on one's laptop computer, the third piece of the monitoring system. See *id.* Essentially, the Charmr looks and functions like a standard flash drive, which is a small storage device that can be inserted via USB connection into the side of any laptop. The difference between the Charmr and a typical flash-drive is that the Charmr's connection with a diabetic's laptop represents a nexus between the interior of the user's body and the hard drive on one's computer. Quite literally, the computer's screen and hard drive capture the functions of the interior of its user's body, and process the information in a way that alerts the user to a recommended course of future actions. Currently, Adaptive Path is waiting for a pharmaceutical company to put the product into production and bring it to market. *Id.* Similarly, in August 2007 a cell-phone-based glucose monitor called GlucoPhone won approval from the FDA. See DARREN MURPH, HEALTHPIA'S GLUCOPHONE GETS FDA APPROVAL (2007), <http://www.engadget.com/2007/08/11/healthpias-glucohone-gets-fda-approval/>. The product consists of a blood glucose meter built into one's cell-phone. The user is able to send results to his doctor over the air after testing himself with the GlucoPack, containing a needle that takes a blood sample. *Id.* For a user of the GlucoPhone, his cell phone becomes a pathway between the interior of his body and his doctor's recommendation.

¹⁷² See Mediquations, <http://www.mediquations.com/index.html> (last visited July 28, 2009). On its homepage, Mediquations states, "for the iPhone and iPod Touch brings over 211 common medical calculations and scoring tools to your fingertips with the simplicity and elegance you expect out of an iPhone application. If you're a health professional, Mediquations is quite possibly the most important companion for your iPhone!" *Id.*

their user can quickly and easily determine if he is having a medical emergency.¹⁷³ Therefore, just by glancing at its user's computer screen, one can, in effect, breach the skin of its owner in real time.

One might argue that searching these devices is no different than searching a box of medical records, which an officer may search at the border without any suspicion. However this argument fails for several reasons. First, the screen of a computer or iPod, reporting information from inside one's body in real time, is no different than looking at an x-ray of the traveler's body, for which some level of suspicion is required even at the border.¹⁷⁴ Second, devices such as the Charmr and GlucoPhone,¹⁷⁵ make future predictions about processes beneath the skin, based on moment-to-moment blood monitoring. A box of documents, reporting the status of one's health hours, weeks, or years before, is not as immediately relevant.

Certainly, these devices are not currently in wide use, so their *current* constitutional significance is minimal. These devices do, however, demonstrate that adhering to the bright line body-property rule in *Flores-Montano* and *Arnold* will generate counterintuitive constitutional results as computer technology advances. Furthermore, these devices will doubtless become more prevalent in years to come. Computers, unlike *any* other containers, have the ability—and will increasingly have the ability—to expose the interior of one's body to an agent of the government. Such a search, performed without any suspicion of illegal activity, certainly will implicate one's person-dignity. As medical technology increases the nexus between the human body and the computer, suspicionless searches will become more and more “nonroutine” and unreasonable, and they will violate the Fourth Amendment.

IV. THE APPROPRIATE BALANCE: “ONE GOOD REASON”

To properly balance the government's interest in protecting the border and an individual's privacy interest in the data inside her laptop, this Note proposes customs officers have “one good reason” to perform invasive data searches. This proposed standard would be greater than no suspicion, but less than a reasonable suspicion¹⁷⁶ or probable

¹⁷³ See DARREN MURPH, CHARMR CONCEPT TRANSFORMS GLUCOSE MONITORING (2007), <http://www.engadget.com/2007/08/15/charm-concept-transforms-glucose-monitoring/> (suggesting that the Charmr is intended for self-monitoring, and has a user-friendly interface).

¹⁷⁴ See *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).

¹⁷⁵ See text accompanying note 165 *supra*.

¹⁷⁶ An officer has a reasonable suspicion where she develops a “particularized and objective basis, supported by specific and articulable facts, for suspecting a person of criminal activity.” BLACK'S LAW DICTIONARY 696 (3d pocket ed. 2006). With this level of suspicion, an officer

cause,¹⁷⁷ the two federal constitutional levels.

Beyond these two levels, customs agents should have more leeway for investigation, and individuals should have more room to protect their privacy. The *CBP Policy*, allowing suspicionless data searches, exemplifies the problem. At the border, a protected environment where officers encounter strangers for the first time, it is difficult for an agent to develop a reasonable suspicion or probable cause. But clearly this cannot mean a customs agent never has the right to search. With respect to searching data inside laptops, the government's solution is eliminating the suspicion requirement entirely. This creates an imbalance of interests, where the government always prevails over the individual. A better solution is to recognize a meaningful middle ground between no suspicion and reasonable suspicion,¹⁷⁸ a middle ground comparable to the standard promulgated by New York Court of Appeals in *People v. De Bour*.¹⁷⁹

In *De Bour*, the Court of Appeals set forth four tiers of permissible police intrusion given facts on the ground: first, "approaching to request information" requires an officer to have an objectively credible reason to ask for a person's identification;¹⁸⁰ second, the "common law right to inquire"¹⁸¹ requires a founded suspicion that criminal activity is afoot

may "stop and frisk" a suspect. *Terry v. Ohio*, 392 U.S. 1, 1, 10 (1968) (holding an officer's stop and frisk constitutional based on reasonable suspicion where the officer observed two men repeatedly peering into a store five or six times).

¹⁷⁷ Probable cause exists where a reasonably trustworthy source alerts an officer to facts "sufficient in themselves to warrant a man of reasonable caution in the belief that . . . evidence subject to seizure will be found in the place to be searched." *DRESSLER & THOMAS, supra* note 14, at 132 (citing *Brinegar v. United States*, 338 U.S. 160 (1949) and *Carroll v. United States*, 267 U.S. 132 (1925)). See also *Illinois v. Gates* 462 U.S. 213 (1983) (holding an officer's arrest constitutional and supported by probable cause based on corroborating information in an anonymous letter that drug dealers would be traveling at particular times in particular cars).

¹⁷⁸ Importantly, in an attempt to create an avenue for permissible police investigation that does not constitute a seizure, many courts have also recognized the need for a standard between no suspicion and reasonable suspicion. In the context of street encounters, these courts typically create this middle standard to allow for *greater* police intrusion for which an officer does not need reasonable suspicion or probable cause. *State v. Boswell*, 294 S.E.2d 287, 294-95 (W.Va. 1982) (holding officer's tapping on suspect's car's window and asking for identification was merely a "minimum intrusion" not constituting a stop, where officer saw suspect turn off the lights in his car when approached late at night near a rowdy bar and near a feed store where arson had been committed); *Atchley v. State*, 393 So. 2d 1034, 1044 (Ala. Crim. App. 1981) (holding defendant was not stopped or seized within the meaning of the Fourth Amendment where officers approached a drunk man sleeping in his car and asked him to identify himself and explain what he was doing) (citing *United States v. Mendenhall*, 446 U.S. 544 (1980)); *State v. Wood*, No. L-77-149, 1977 WL 198670, at *1-2 (Ohio Ct. App. Dec. 23, 1977) (holding officer's approaching suspect at a location known for illegal gambling and asking him about potentially stolen goods was not a seizure under the Fourth Amendment) (citing the balancing test set forth in *Camara v. Municipal Court*, 387 U.S. 523 (1967)).

¹⁷⁹ *People v. De Bour*, 40 N.Y.2d 210 (1976).

¹⁸⁰ *Id.* at 223.

¹⁸¹ *Id.*

before an officer can ask probing questions like “what’s in the bag?”¹⁸² or “what are you doing in this neighborhood?”¹⁸³ The two highest tiers are reasonable suspicion and probable cause.¹⁸⁴

De Bour and *People v. Hollman*¹⁸⁵ clarify what facts must be known to allow for some police intrusion where an officer does not have reasonable suspicion to stop a suspect or probable cause to arrest. These kinds of facts¹⁸⁶ that establish “founded suspicion” correspond, in effect, to “one good reason.”

While *De Bour* governs New York street encounters, its four-tiered system would be helpful in the border search context where data is concerned. In this context, the facts representing each tier would be instructive to customs agents, but the levels of intrusion warranted by each tier would shift as follows. Tier one would be irrelevant because every encounter between a customs agent and a traveler is like a stop on the street. Tier two, however, would be the critical tipping point below which an agent would not be allowed to invasively search a traveler’s data. Where an agent observed tier-two-type facts,¹⁸⁷ however, she would have “one good reason” to search the traveler’s data.

Adopting this standard would increase efficiency at the border by ensuring that certain time-consuming and ineffective *bad* reasons fall below the standard. Such reasons would include basing searches on an agent’s mere “whim or caprice,”¹⁸⁸ harassing a bothersome traveler,¹⁸⁹ or basing a search solely on racial profiling.¹⁹⁰ Problematically, the

¹⁸² *People v. Hollman*, 79 N.Y.2d 181, 189-90 (1992).

¹⁸³ *De Bour*, 40 N.Y.2d at 213-14.

¹⁸⁴ *Id.* at 223.

¹⁸⁵ 79 N.Y.2d 181.

¹⁸⁶ In *De Bour*, an officer asked a man what he was doing in the neighborhood late at night after witnessing him cross the street when he saw the officer approaching. The suspect answered clearly but nervously. 40 N.Y.2d at 213. The Court of Appeals held these facts insufficient to support a reasonable suspicion, yet sufficient to rise to the second level, a founded suspicion that criminal activity was afoot. *Id.* at 224-26. The Court of Appeals held similarly in *Hollman* that a tier two inquiry was permissible where an officer witnessed two men carrying bags through a bus terminal, switching bags in the bathroom, boarding a bus, and checking their bags several seats in front of them. *Hollman*, 79 N.Y.2d at 192-93. When the officer asked where the men were traveling, if they knew each other, and if they owned the bags, the men answered they were traveling to different states, had never met before boarding the bus, and denied ownership of their luggage. *Id.* at 193. The Court of Appeals found these probing questions constitutional, supported by the second level of suspicion, even though they did not give rise to a reasonable suspicion. *Id.* at 193-94. Finally, in contrast, in a companion case to *Hollman*, the Court of Appeals found the facts alleged by the officer rose to level one but not level two where the officer merely witnessed a man who “appeared nervous, scanning the interior of the [bus] boarding area.” *Id.* at 187.

¹⁸⁷ Examples of tier-two-type facts are set forth in note 186.

¹⁸⁸ *De Bour* itself protects against harassment based on an agent’s “whim or caprice,” suggesting core Fourth Amendment protection is rooted in freedom from “all arbitrary intrusions by the government.” *Id.* at 217-19.

¹⁸⁹ See *supra* note 133.

¹⁹⁰ *People v. Lopez*, 864 N.Y.S.2d 696, 699-702 (Kings County, Sup. Ct. 2008) (citing

current *CBP Policy*, permitting data searches without justification, allows searches for all these bad reasons, compromising efficiency and border security.¹⁹¹ A look at the computer search cases discussed in Part I.D *supra* demonstrates how this proposed standard would operate practically in the field.

In *Romm*, where Canadian customs agents told their U.S. counterparts that the defendant had child pornography on his computer,¹⁹² the officers certainly had one good reason to search his computer's data for further contraband. In *Ickes*, where the officer discovered photographs of nude children in defendant's van as he crossed the Canadian border,¹⁹³ the officer likewise had one good reason to believe defendant's computer files may contain further contraband. In contrast, in *Arnold* where the officer knew only that the defendant had traveled to the Philippines,¹⁹⁴ she did not have one good reason to search the data on defendant's laptop.

Taking the facts from the New York street encounter cases discussed *supra* and putting them into the border context is also helpful in illustrating the workability of the "one good reason standard." As in *Hollman*, if an officer observed two associates switch bags, then abandon them just before entering U.S. customs,¹⁹⁵ the agents would have one good reason to search any data in the computers the bags may contain. Likewise, as in *De Bour*, where a person backed away from the officers after being spotted glancing around nervously,¹⁹⁶ an officer would have one good reason to search the suspect's data inside his computer. But where an officer witnessed a traveler merely appearing nervous, without more, the officer would not have a good reason to perform an invasive data search, and the search would be unreasonable.

Therefore, where an officer witnesses tier-two-type facts, similar to those in *De Bour* and *Hollman*, she would have one good reason to search the data in a traveler's computer. This standard strikes the appropriate balance between the government's interest in protecting the

statistical studies that have confirmed the claim that minorities are much more likely to be stopped by the police). One of the studies cited in *Lopez* lends credence to the argument that racial profiling is an inefficient use of time and police resources. See Jeffrey Fagan, *An Analysis of the NYPD's Stop-and-Frisk Policy in the Context of Claims of Racial Bias*, at 14 (Columbia Law Sch. Pub. Law & Legal Theory Working Paper Group Paper No. 0595, 2004), available at <http://lsr.nellco.org/cgi/viewcontent.cgi?article=1019&context=columbia/pllt> ("[S]tops of whites are more 'efficient' and are more likely to lead to arrests, whereas for blacks and hispanics, the police are stopping more indiscriminately, and fewer of the people stopped in these broader sweeps are actually arrested.").

¹⁹¹ See *supra* Part II.A (arguing that searching where there is no risk of harm compromises border safety).

¹⁹² *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006).

¹⁹³ *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005).

¹⁹⁴ *United States v. Arnold*, 533 F.3d 1003, 1005 (9th Cir. 2008).

¹⁹⁵ *People v. Hollman*, 79 N.Y.2d 181, 185-86 (1992).

¹⁹⁶ *People v. De Bour*, 40 N.Y.2d 210, 213 (1976).

border and an individual's interest in privacy.

CONCLUSION

Considering both the inefficiency concerns associated with allowing customs officers to search data without one good reason and the numerous individual privacy concerns implicated in such border searches, the individual's interest should prevail where an agent has no good reason to search a traveler's laptop. The *CBP Policy* allowing suspicionless searches should be found to violate the Fourth Amendment.

This view would not require overturning any Supreme Court precedent, because, as this Note has argued, the data inside laptops falls outside the scope of the border search and special needs doctrines, and the Court has never held otherwise. Therefore, the Court should not apply lopsided special needs balancing to invasive data searches performed at the border. Instead, the Court should apply *Terry* balancing, meaningfully considering both the government's interest in protecting its borders and an individual's interest in privacy. Requiring a customs agent to have one good reason to search the data inside a traveler's computer appropriately strikes this balance and prevents time-consuming fishing expeditions that may compromise border security. The *CBP Policy* in its current form should be discarded.