8-2016

Border Search Exception: Historical Underpinnings, Present Challenges, Critical Importance

Jeffrey A. Vent

APUS Library Capstone Submission Form

This capstone has been approved for submission to and review and publication by the APUS Library.

Student Name [Last, First, MI] *	Vent		Jeffrey
Course Number [e.g. INTL699] *	LSTD 699	**Paper Date** [See Title pg.]	June 2016
Professor Name [Last, First] *	Ekman, Christina E.		
Program Name * See list	Legal Studies		
Keywords [250 character max.]	Fourth Amendment; Border Search Exception; "Mobile Technology Devices"		
Passed with Distinction * Y or N	Y		
Security Sensitive Information * Y or N	N		
IRB Review Required * Y or N	N		
Turnitin Check * Y or N	Y		

If YES, include IRB documents in submission attachments.

All capstone papers must be checked via Turnitin.

* Required

Capstone Approval Document

The thesis/capstone for the master's degree submitted by the student listed (above) under this title *

Border Search Exception: Historical Underpinnings, Present Challenges, Critical Importance

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit to the amount of 3 semester hours.

Program Representatives	Signatures	Date (mm/dd/yyyy)
Signed, 1st Reader * [capstone professor]	Christina E. Ekman	06/28/2016
Signed, 2nd Reader (if required by program)		
Recommendation accepted on behalf of the program director *	Terri L. Wilkin	6/30/2016
Approved by academic dean *	Digitally signed by mriccardi@apus.edu DN: cn=mriccardi@apus.edu Date: 2016.09.05 20:12:55 -06'00'	

* Required

BORDER SEARCH EXCEPTION: HISTORICAL UNDERPINNINGS, PRESENT CHALLENGES, CRITICAL IMPORTANCE

A Masters Capstone Project Paper

Submitted to the Faculty

of

American Military University

by

Jeffrey A. Vent

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Arts

June 2016

American Military University

Charles Town, WV

The author hereby grants the American Public University System the right to display these contents for educational purposes.

The author assumes total responsibility for meeting the requirements set by United States copyright law for the inclusion of any materials that are not the author's creation or in the public domain.

Special Note: Although the author is an employee of the United States Government, this is solely a student submission in partial fulfillment of the requirements for an academic degree. Nothing in this paper should be construed to be the official position of U.S. Customs and Border Protection, the Department of Homeland Security, or the United States Government. The sources used in this paper are completely in the public domain and any apparent positions should be considered those of the author alone.

DEDICATION

To my parents, whose endless wisdom and encouragement have kept me striving for greater heights. I love you both!

-AND-

To my brothers and sisters of the Thin Blue Line. Together, we are all that stands between the evil and the innocent.

ACKNOWLEDGEMENTS

I wish to thank Christina Ekman, J.D., LL.M., for her continuous help and guidance throughout the writing process. Her mastery of the law (and the Bluebook) has repeatedly demonstrated her dedication to her craft. Her expertise and feedback were immensely helpful and will never be forgotten.

I also wish to thank American Military University, its staff, and all of my professors from the Legal Studies program. They have opened my eyes to the depth and complexity of the law, and renewed my interest in lifelong learning.

ABSTRACT OF THE PROJECT

BORDER SEARCH EXCEPTION: HISTORICAL UNDERPINNINGS, PRESENT CHALLENGES, CRITICAL IMPORTANCE

by

Jeffrey A. Vent

American Public University System, June 19, 2016

Charles Town, West Virginia

Professor Christina Ekman, J.D., LL.M., Project Professor

This paper examines the historical underpinnings, present challenges, and the critical importance of the border search exception to the warrant requirement imposed by the Fourth Amendment. The paper begins with a look at the history of the border search exception and traces it to modern day statutory law. The border search exception as it applies to electronic media is then examined to include current case law. Present challenges, or arguments against suspicionless electronic media searches, are presented and refuted. Further, arguments for maintaining a lack of individualized suspicion to conduct these searches are also explored. Finally, a brief examination of the border search laws of the United Kingdom and Canada is conducted. Ultimately, the point of the paper is to argue that despite an increase in technology, the border search exception should not be modified to create an exception for electronic media devices by requiring particularized suspicion.

TABLE OF CONTENTS

I. Introduction

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[1] The first twenty-four words of a Constitutional Amendment only fifty-four words in length, this statement from the Fourth Amendment provides sweeping protection against unreasonable government searches of our persons and property.[2] The remainder, or the second part, of the Fourth Amendment contains a warrant clause, commanding that searches be conducted only with a warrant that is supported by probable cause, therefore subjecting the facts to judicial review and specifically limiting the scope of the intrusion.[3]

Is it assumed, therefore, that absent a warrant a search is *per se* unreasonable? In the absence of Fourth Amendment jurisprudence, this would likely be the case, however, with time courts have carved out a number of exceptions to the warrant requirement. For example, one may be stopped on the street for an investigation without a warrant and on less than probable cause,[4] and one may be frisked for weapons upon an articulable belief that the person stopped is "armed and presently dangerous."[5] Further, with what has become known as the hot pursuit exception,

---

[1] U.S. CONST. amend. IV.

[2] *Id.*

[3] *See* Luis G. Stelzner, *The Fourth Amendment: The Reasonableness and Warrant Clauses*, 10 NEW MEX. L. REV. 33, 48 (1979).

[4] Terry v. Ohio, 392 U.S. 1, 44 Ohio Op. 2d 383 (1968).

[5] *Terry*, 392 U.S. at 24.

private property may be entered when law enforcement is in hot pursuit of a fleeing felon.[6]

Another such exception to the warrant requirement is the border search exception.[7] This exception recognizes that warrantless and suspicionless searches conducted at the border are *per se* reasonable solely by virtue of the fact that they occur at the border.[8] As will be discussed below, the courts have not hesitated to affirm this plenary search authority throughout a long history of case law. However, with an increase in the use of mobile technology devices, and the transiting of those devices across the international border, the border search exception now faces challenges from opponents who believe that it should not apply to these items. These opponents are demanding a higher standard of suspicion before searches of these devices, or electronic media, may be conducted.[9] To that end, this paper will investigate the arguments these opponents make, and examine them against the backdrop of the history of the border search exception, current case law, and logical argument; while convincing the reader that allowing an exemption for these devices would be a poor policy decision.

---

[6] Warden v. Hayden, 387 U.S. 294, 298 (1967).

[7] The terms border search exception and border search authority will be used interchangeably in this paper. They refer to the same thing as the exception itself permits the authority to be exercised.

[8] Yule Kim, PROTECTING THE U.S. PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT 1 (Congressional Research Service, 2009). She notes in this article that there are two distinct types of searches; routine, which requires no articulable suspicion and non-routine, which may require some articulable suspicion.

[9] Because technology devices are forms of "electronic media," this term will be used throughout this paper to refer to both digital data and the devices that read and write it.

To accomplish this, this paper will be comprised of several parts. In part II this paper will examine the function, history, and evolution of the border search exception through case law and statutes. In part III, case law specifically addressing these electronic media searches will be reviewed, as well as the policy established for these searches by Customs and Border Protection, one of the agencies that conducts them. In part IV, some of the arguments made by opponents to these suspicionless electronic media searches will be introduced and discussed. In part V, this paper will present argument as to why granting these demands for a higher suspicion standard for electronic media searches would be dangerous and could, therefore, subject the United States to undue risk. Finally, in part VI an examination of the border search laws of two other developed countries that are on par with the United States will be introduced and compared to the laws here.

By the end of this paper, the reader will have achieved an understanding of not only the history of the border search exception, but the challenges it presently faces with the increase in technology, and why the exception is critically important to the security of the United States.

II. Border Search Exception – Function, History, Evolution

This part will address the purpose and functionality of the border search exception, as well as its history and evolution. In this part, the reader will travel back a few hundred years, to the creation of the border search exception, and follow along as the courts examine the border search authority and affirm its necessity and function. Next, this part will address the modern day statutory authorities that permit the border

search exception to be exercised. Finally, this part will address how electronic media, as it continues to become more prevalent in people's lives, has been affected by the border search exception.

A - Function and Purpose of the Border Search Exception

As mentioned above, Fourth Amendment jurisprudence has carved out a number of exceptions to the warrant requirement.[10] These exceptions vary in their scope but generally serve as an exception to the requirement to obtain a warrant before conducting a search.[11] For example, as noted above, the hot pursuit exception allows an officer in hot pursuit of a fleeing felon to enter private property without a warrant.[12] A search that is conducted outside of a valid exception and without a warrant is generally considered unreasonable, and in violation of the restrictions imposed on the government by the Fourth Amendment.[13] Numerous examples of this may be found throughout Fourth Amendment case law; such as the warrantless search of a rented home solely on the landlord's authorization upon smelling whiskey mash,[14] or the illegal search of a hotel room after police officers smelled burning opium emitting into the

[10] *Fourth Amendment*, CORNELL UNIVERSITY LAW SCHOOL – LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/fourth_amendment (last visited Apr. 2, 2016).

[11] *Id.*

[12] *Warden,* 387 U.S. at 294.

[13] *Fourth Amendment*, CORNELL UNIVERSITY LAW SCHOOL – LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/fourth_amendment (last visited Apr. 2, 2016).

[14] Chapman v. United States, 365 U.S. 610 (1961).

hallway.[15] In both of those cases, the courts found that there could be no exception that justified the searches as this was exactly the type of abuse that was meant to be prevented by the Fourth Amendment.

"But a port of entry is not a traveler's home."[16] Therefore, as one of the exceptions recognized through Fourth Amendment jurisprudence, and the focus of this paper, the border search exception is a general exception that renders warrantless searches at the border as *per se* reasonable solely because they occur at the border.[17] Pursuant to this exception and statutory authority, which will be addressed shortly, Customs and Border Protection (CBP) Officers have broad authority to conduct these border searches.[18]

The purpose behind the border search exception is to allow for the United States, as a sovereign nation, to protect itself from the entry of unwanted persons and items.[19] In a number of decisions, the courts have ruled that this is a permissible function because it facilitates the collection of duties as well as preventing the introduction of contraband into the country.[20] This protection function is enabled by the plenary

---

[15] Johnson v. United States, 333 U.S. 10 (1948).

[16] United States v. Thirty-Seven Photographs, 402 U.S. 363 (1971).

[17] Kim, *supra* note 8, at 1.

[18] *CBP Search Authority*, U.S. CUSTOMS AND BORDER PROTECTION, http://www.cbp.gov/travel/cbp-search-authority (last visited Apr. 2, 2016).

[19] Judith B. Ittig, *The Rites of Passage: Border Searches and the Fourth Amendment*, 40 TENN. L. REV. 329 (1973).

[20] *Montoya de Hernandez,* 473 U.S. at 537-538. Relying on Carroll v. United States, 267 U.S. 132, 154 (1925).

authority to "conduct routine searches and seizures at the border, without probable cause or a warrant."[21] As Judith Ittig writes, the inspection process would be "almost completely frustrated" by the need for the officers conducting an inspection to show probable cause and obtain a warrant.[22] She further states that there is typically no advance knowledge of a traveler or the items they bring before their inspection.[23] Because the inspections must occur at a rapid pace, and without this foreknowledge, in the absence of broad search authority Customs might be left to take travelers' words as to what they were bringing into the country and that both they, and their items, are admissible.[24] Logically, because the security of the country is at stake, officers cannot simply assume everyone is truthful when they enter and exit the United States.

Not only is the border search exception a very powerful exception to the warrant requirement of the Fourth Amendment, it also has a deep rooted history in our nation's laws. The next section addresses this deep rooted history, from the inception of the border search exception to modern day.

B - The Creation of the Border Search Exception

The border search exception (authority) derives from one of the first acts of the First Congress.[25] The year is 1789 and the First Congress has just successfully

---

[21] *Montoya de Hernandez,* 473 U.S. at 537.

[22] Ittig, *supra* note 19 (page numbers omitted).

[23] *Id.*

[24] *Id.*

[25] Act of July 31, 1789, ch. 5 § 24, 1 Stat. 29, 43.

accomplished the ratification of the new United States Constitution (June 1788).[26] In this post-Revolutionary War era, the fledgling United States badly needed revenue to pay the debts incurred in fighting the war as well as the mounting government operating costs.[27] One of the country's founding fathers, Alexander Hamilton, argued on numerous occasions in the Federalist Papers that the national debt could be battled by an incoming revenue stream generated from, amongst other things, taxes or duties on imported items.[28] In Federalist Number 12, Hamilton argued that "a nation cannot long exist without revenues. Destitute of this essential support, it must resign its independence, and sink into the degraded condition of a province."[29]

The First Congress apparently feared Hamilton was correct and in agreement with his logic established, in one of its first acts, the Customs Service.[30] Customs was tasked with collecting the manifests of all items imported, calculating and assessing appropriate duties, and collecting the same.[31] Because these duties were taxes on items that may not have been taxed previously, it was logical that not everyone could be expected to be forthcoming about their imports. Therefore, paramount to ensuring the

---

[26] *The Ratification of the Constitution*, NATIONAL ARCHIVES, http://www.archives.gov/education/lessons/constitution-day/ratification.html (last visited Apr. 4, 2016).

[27] *History,* NATIONAL U.S. CUSTOMS MUSEUM FOUNDATION, http://customsmuseum.org/history (last visited Apr. 2, 2016).

[28] *Id. See also*, THE FEDERALIST NO. 12, (Alexander Hamilton).

[29] THE FEDERALIST NO. 12. (Alexander Hamilton).

[30] Act of July 31, 1789, ch. 5, 1 Stat. 29.

[31] *Id.*

collection of accurate duty was the ability to search all incoming vessels for dutiable items. To accomplish this, in that same act, Congress granted Customs the ability to enter all incoming vessels and search for dutiable items.[32] Further, the authority to seize and forfeit items that were not reported or found to differ from what was manifested, was delegated.[33]

At the time of passage of the act, the Fourth Amendment did not yet exist and would not be proposed until two months later.[34] Judith Ittig notes that the historical significance of this chain of events may indicate that the same legislature who proposed the Bill of Rights, "did not intend the Fourth Amendment to be fully applied to the customs power," as the ability for Customs to conduct searches was already established.[35] A year after the passage of the Act of July 31, 1789, Congress would revisit the issue and pass an updated but relatively similar act. As a part of the Act of August 4, 1790, Customs retained its vessel search authority, but it was also expanded to allow for the boarding of vessels before they even reached the coast of the United States.[36]

The creation of Customs turned out to be a very beneficial decision for the new nation, as the revenue collected over the next century, in addition to helping pay for the

[32] Act of July 31, 1789, ch. 5 § 24, 1 Stat. 29, 43.

[33] *Id.*

[34] Ittig, *supra* note 19 (page numbers omitted).

[35] Ittig, *supra* note 19 (page numbers omitted).

[36] Act of August 4, 1790, ch. 35 § 31, 1 Stat. 164.

debts incurred in the Revolutionary War, helped the new nation to expand by acquiring land, and to build the epicenter of the Federal Government at Washington D.C.[37]

C - Building a History

In the Act of March 3, 1815, the Thirteenth Congress again visited the issue of customs inspections.[38] Congress again authorized the power to enter ships, vessels, boats, or rafts to search for any items subject to duty where there was an attempt to evade the payment thereof, or any items that were being imported contrary to the laws of the United States.[39] In addition, in the next section, Congress granted the authority for Customs inspectors and surveyors to stop any person on foot, in a vehicle or carriage, or on any "beast of burden" to conduct the same inspections.[40] Regardless of what type of stop was made, and regardless of whether the intent had been to introduce illegal items or to evade duties, the inspectors had the authority to seize and secure the items for trial.[41] The bulk of this authority would eventually morph into Section 3061 of the Revised Statutes.[42]

---

[37] *History,* NATIONAL U.S. CUSTOMS MUSEUM FOUNDATION, http://customsmuseum.org/history (last visited Apr. 2, 2016).

[38] Act of March 3, 1815, ch. 94 § 1, 3 Stat. 231.

[39] *Id* at 232.

[40] Act of March 3, 1815, ch. 94 § 2, 3 Stat. 232.

[41] Act of March 3, 1815, ch. 94 § 1&2, 3 Stat. 231-232.

[42] Now codified as 19 U.S.C. 482(a). Statutory history cited in Carroll v. United States, 267 U.S. 132, 152 (1925).

It was inevitable with the passage of time that a border search would reach the judiciary. One of the earliest cases involving the exception was *Cotzhausen v. Nazro.*[43] In *Cotzhausen* a scarf was imported from Germany through the international mail in violation of the treaty of Berne of October 9, 1874.[44] That treaty prohibited the importation of any articles through the mail which may be subject to duties.[45] Upon the arrival of the scarf in Milwaukee, Customs officer Nazro seized the scarf, leading to the case.[46] In its ruling, the Court recognized that compelling every passenger who lands in the United States to complete a declaration and subjecting them to inspection would be to no avail if the customs process could be subverted by simply sending dutiable items through the international mails.[47] The Court ruled that Nazro had fulfilled his duty as an officer of Customs and refused to reverse the judgment of the lower court.[48] This was, essentially, recognition by the Court that the customs process was important to the United States, and subverting it could not be permitted.

Just over forty years later, in 1925, the Supreme Court would decide on *Carroll v. United States* touching, in its opinion, on searches conducted at the border and setting them apart from searches conducted in the interior of the country.[49] "Travellers may be

---

[43] Cotzhausen v. Nazro, 107 U.S. 215 (1883).

[44] *Id* at 217.

[45] *Id.*

[46] *Id.* at 215-216.

[47] *Id.* at 218.

[48] *Id.* at 220.

[49] Carroll v. United States, 267 U.S. 132 (1925).

so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in and his belongings as effects which may be lawfully brought in."[50] Although *Carroll* did not address a border search, the Court seized the opportunity to comment on the distinction between the two types of searches, clearly indicating, even 135 years after the creation of the border search authority, that border searches are searches of a distinct caliber.

Fast forward another fifty years, and *United States v. Ramsey* arrives at the Supreme Court.[51] *Ramsey* involved the attempted importation of heroin through the international mail.[52] An astute Customs inspector noticed eight envelopes from Thailand that were bulky and that potentially contained merchandise.[53] Having what the Court would later call "reasonable cause to suspect" that was established by the origin of the envelopes, their weight, and their appearance; the inspector opened the envelopes and discovered Heroin.[54] The Court determined that this action was plainly within the meaning of the authorizing statute and then turned to whether, despite the statutory authorization, the search was forbidden by the Constitution.[55] The Court returned to their decision in *Cotzhausen* and reaffirmed that no difference may be

[50] *Carroll*, 267 U.S. at 154 (Misspelling in original).

[51] United States v. Ramsey, 431 U.S. 606 (1977).

[52] *Id.*

[53] *Id.* at 609.

[54] *Id.* at 609-610.

[55] *Id.* at 611-615.

recognized as to mode of transportation when it comes to the applicability of border search authority.[56] The Court further recognized that a long history of jurisprudence had recognized the "plenary customs power" to "stop and examine persons and property crossing into this country."[57]

Ten years later, in the 1980's, the Supreme Court would again hear a significant case related to a border search when it considered *United States v. Montoya de Hernandez.*[58] In *Montoya de Hernandez* a woman traveling from Colombia was referred for a secondary customs inspection after arriving in Los Angeles.[59] During secondary inspection, Customs inspectors found inconsistencies between her stated purpose of travel and her plans while in the United States, the amount of currency she was carrying, a lack of hotel reservations, an inability to recall how she purchased her airline ticket, and clothing inappropriate for the weather.[60] These factors led the Customs inspectors to believe that Montoya de Hernandez was smuggling narcotics in her alimentary canal.[61] A patdown revealed no contraband, but the female inspector who conducted the patdown indicated that the subject's abdomen was very firm.[62]

---

[56] *Id.* at 620-621.

[57] *Id.* at 616.

[58] United States v. Montoya de Hernandez, 473 U.S. 531 (1985).

[59] *Id.*

[60] *Id.* at 533-534.

[61] *Id.* at 534. The alimentary canal covers the entire route through which food passes after consumption.

[62] *Id.*

Given the indicators, Montoya de Hernandez was offered three options; to take an x-ray at the hospital, to produce a monitored bowel movement, or to return to Colombia on the next available flight.[63] After consenting and then withdrawing her consent to the x-ray, she elected to return to Colombia.[64] After it was determined that no flights were available for her to return to Colombia, she was told she would either need to consent to the x-ray or would be detained until she moved her bowels.[65] Over the time of her detention, the subject refused food and drink and refused to use the restroom even, as the Court called it, exhibiting "symptoms of discomfort consistent with heroic efforts to resist the usual calls of nature."[66] Eventually, Customs sought a court order authorizing a rectal exam and x-ray, and a physician acting on that order removed a balloon containing a foreign substance from the subject's rectum.[67] Over the course of several days Montoya de Hernandez passed a total of eighty-eight balloons containing Cocaine.[68] In its opinion, the Court recognized the longstanding plenary border search power.[69] However, this was also a defining case for the border search authority as it marked the point at which the Court determined that although the Fourth Amendment balance is struck far more favorably to the government at the border, some searches

---

[63] *Id.*

[64] *Id.* at 535.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.* at 537.

simply cannot be considered routine and that non-routine searches may require a level of suspicion.[70] The Court noted that such non-routine searches include "strip, body-cavity, or involuntary x-ray searches," but declined to indicate what level of suspicion may be necessary for those searches.[71]

After the turn of the century the Supreme Court would hear another significant border search case, and would clarify slightly the opinion in *Montoya de Hernandez*. In *United States v. Flores-Montano*, Customs officers seized thirty-seven kilograms of Marijuana from the gas tank of a Ford Taurus that Flores-Montano attempted to drive through the Otay Mesa Port of Entry in California.[72] After his conviction and on appeal, the Ninth Circuit reversed, stating that the search of the defendant's fuel tank required reasonable suspicion.[73] The Supreme Court reversed again, clearly stating that reasonable suspicion was not required for the search of a fuel tank.[74] The Court returned to its opinion in *Montoya de Hernandez* and stated that although there are "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" that such requirements could not be applied to vehicles.[75] The Court further

[70] *Id.* at 540-542. *See also,* Kim, *supra* note 8, at 1.

[71] *Id.* at 541.

[72] United States v. Flores-Montano, 541 U.S. 149 (2004).

[73] *Id.* at 150.

[74] *Id.*

[75] *Id.* at 152.

reiterated its position from *Montoya de Hernandez* with regard to privacy at the border and held that "the expectation of privacy is less at the border than it is in the interior."[76]

Summarily, the legislative and judicial history of the border search exception indicate that no suspicion is required for routine searches of persons and vehicles while non-routine searches of a person, such as an x-ray, strip search, or body cavity search, may require some level of particularized suspicion.

D – Modern Day Border Search Exception – Statutory Authorities

Having observed the legislative and judicial history of the border search exception, the question becomes what statutes authorize border searches today? A number of statutes that work together to allow Customs and Border Protection the ability to exercise the border search authority will be covered in this section. As the agency born of the 2003 combination of the U.S. Customs Service, the Immigration and Naturalization Service, and other agencies, Customs and Border Protection (CBP) is the agency now responsible for conducting customs, immigration, and agriculture inspections.[77] As part of CBP's staff, CBP Officers act as both immigration officers and customs inspectors at 328 ports of entry into the United States.[78] These officers are empowered to exercise the statutes found in Title 8, United States Code, and Title 19, United States Code, both of which contain search authorities.

---

[76] *Id.* at 154.

[77] *CBP Through the Years,* U.S. CUSTOMS AND BORDER PROTECTION, http://www.cbp.gov/about/history (last visited Apr. 7, 2016).

[78] *CBP Officer*, U.S. CUSTOMS AND BORDER PROTECTION, http://www.cbp.gov/careers/join-cbp/which-cbp-career/cbp-officer (last visited Apr. 7, 2016).

D.1 – Title 19 Statutes

The primary statute that enables Customs to perform border searches, under the applicable exception, is 19 U.S.C. 482.[79] This statute contains nearly the same language as the section of the Act of March 3, 1815 that was covered above.[80] The statute authorizes the stop and inspection of any vessels, vehicles, beasts, or persons "on which or whom" there may be items subject to duty or items introduced "in any manner contrary to law."[81] Further, the opening of any trunk or envelope, regardless of where it is located, upon "a reasonable cause to suspect there is merchandise which was imported contrary to law," is explicitly authorized.[82] Any merchandise that is found in violation of this act is to be seized and secured for trial.[83]

Another statute of significant influence is 19 U.S.C. 1496, which authorizes baggage examinations.[84] These examinations may be made to determine what articles are carried within and whether they are dutiable, duty free, or prohibited.[85]

---

[79] 19 U.S.C. § 482(a) (2012).

[80] In the discussion on the history of the border search exception, the Act of March 3, 1815 was briefly examined. In *Carroll,* 267 U.S. at 152 the Court touched on this act and noted that it later became Section 3061 of the revised statutes. The bulk of that language is now 19 U.S.C. § 482(a).

[81] 19 U.S.C. § 482(a) (2012).

[82] *Id.*

[83] *Id.*

[84] 19 U.S.C. § 1496 (2012).

[85] *Id.*

Additionally 19 U.S.C. 1461, while similar to section 1496, bears mentioning here due to the fact that it covers the search of trunks, other containers, and closed vehicles.[86] Further, it requires that keys be provided to any closed item so that it may be opened for inspection.[87] This particular section will be significant later in the paper (containers).

Finally, 19 U.S.C. 1581 is of significance as it allows officers of Customs to board vessels and vehicles at "any place in the United States or within the customs waters or, as he may be authorized, within a customs-enforcement area established under the Anti-Smuggling Act."[88] Officers are authorized under this statute to examine and inspect the conveyance as well as persons and cargo on board, regardless of where located.[89] This statute also sets forth penalties for various infractions such as false documents and failure to stop.[90]

D.2 – Title 8 Statutes

The vast majority of the border search statutes derive from Title 19, as that applies to customs laws, while Title 8 applies to immigration. However, there is one major statute within Title 8 that grants a significant amount of search authority. The statute is 8 U.S.C. 1357 and the applicable section addresses warrantless searches of a

[86] 19 U.S.C. § 1461 (2012).

[87] *Id.*

[88] 19 U.S.C. § 1581(a) (2012).

[89] *Id.*

[90] *Id.* at (c) and (d).

person who is seeking admission to the United States, as well as all personal effects in that person's possession.[91] There is however, a caveat, in that the officer must have reasonable cause to suspect that "grounds exist for denial of admission to the United States . . . which would be disclosed by such search."[92] Although this is not a difficult standard to meet, at the time this statute was written, immigration officers had no need to search persons who were admissible to the United States as that job was left to the Customs inspectors. Therefore, in the absence of suspicion regarding an immigration violation, the immigration inspector could have relayed any other suspicion to the Customs inspectors.

D.3 – Statutory Summary

Although the vast majority of the border search statutes derive from Title 19, while only one is from Title 8, because the CBP Officer position now encompasses the enforcement of both of those titles of United States Code, the statutes mesh together to create the statutorily authorized modern border search authority.

E - Technology Takes on a Role

Because the general point of this paper is to examine and refute arguments against the suspicionless searches of electronic devices, at this point it is important to demonstrate how profoundly important technology has become in modern life. Think back for a moment at the last time you spoke with someone who did not have a cell phone, or even a laptop computer, for that matter. The odds are that the vast majority

[91] 8 U.S.C. § 1357(c) (2012).

[92] *Id.*

of folks know few others in modern day who do not have at least one type of mobile electronic device, whether that is a cell phone or smartphone, a tablet computer, or a laptop computer.

In January 2016, 198.5 million people in the United States owned smartphones.[93] By comparison, in July 2015, the Central Intelligence Agency listed the population of the United States at 321.3 million.[94] Assuming that the smallest of children and the most elderly of adults probably do not own smartphones, it is clear how prevalent they are in our society.

In 2014, eighty-two percent of U.S. Households had a laptop computer.[95] In January 2014, forty-two percent of American adults owned a tablet computer.[96] For 2016, 202 million laptops and 375 million tablets are expected to be shipped worldwide, while only 127 million desktops are predicted to be shipped.[97] For reference, in 2010, 157 million desktops shipped while laptops were roughly the same and only 19 million

---

[93] COMSCORE REPORTS JANUARY 2016 U.S. SMARTPHONE SUBSCRIBER MARKET SHARE (Mar. 3, 2016), http://www.comscore.com/Insights/Rankings/comScore-Reports-January-2016-US-Smartphone-Subscriber-Market-Share.

[94] *The World Factbook-United States,* CENTRAL INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (last visited Apr. 13, 2016).

[95] *Digital Democracy Survey*, DELOITTE (Ninth Ed. 2014), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-deloitte-democracy-survey.pdf.

[96] *Mobile Technology Fact Sheet*, PEW RESEARCH CENTER, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/#.

[97] *Shipment forecast of tablets, laptops, and desktop PCs worldwide from 2010 to 2019*, http://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/.

tablets were shipped.[98] These statistics demonstrate that mobile technology is growing and is taking over territory that was likely held by non-mobile technology in the past.

The point of these statistics is rather simple. Because mobile technology continues to increase and travelers have the ability to take these mobile devices with them when they travel, whether domestically or internationally, they likely do. Logically this implies that searches conducted at the border will encounter more and more of these devices moving forward, and they may contain information which was stored another way in the past (such as a journal or photo album). This leads to part III, and border searches of electronic media.

III. Border Searches of Electronic Media at Present

In this part, the paper will examine some of the judicial history regarding border searches of electronic media, arriving at their current state. Additionally, the policy that governs the authority of Customs and Border Protection to conduct these electronic media searches will be examined.

A – Judicial Decisions on Border Searches of Electronic Media

One of the early cases involving an electronic media search occurred in 2003, in the United States District Court for the Southern District of New York. In *United States v. Irving*, defendant Stefan Irving was stopped while re-entering the U.S. from Mexico at

[98] *Id.*

Dallas-Fort Worth International Airport.[99] Customs agents had previously advised inspectors working at the airport that Irving was under investigation for sex crimes involving children and therefore asked the inspectors, upon encountering Irving, to conduct a search of his luggage.[100] After the search of Irving's luggage, which revealed children's books and drawings, the investigating agents asked to speak with Irving.[101] During this discussion, the agents again searched the luggage and found diskettes and undeveloped film, which Irving was told would be checked for child pornography and returned to him if it contained no such thing.[102] The film contained nothing of concern but the diskettes were found to contain "images of child erotica," and the government subsequently indicted Irving.[103] In its discussion, the court noted that several other courts had compared notebook computers to closed containers and determined that the diskettes were likewise closed containers.[104] The court opined that if an exemption were made for the diskettes, persons crossing the border would be able to immunize information to search solely by putting it on a diskette.[105] This is an important point, as it recognizes that the court remained with the history of jurisprudence of refusing to

---

[99] United States v. Irving, 2003 U.S. Dist. LEXIS 16111 (S.D.N.Y. 2003). The case and resulting opinion were the result of a motion to suppress filed by Irving with regard to the diskettes, film, and statements he made during the interview.

[100] *Id.* at 2.

[101] *Id.* at 3-4.

[102] *Id.* at 5.

[103] *Id.* at 6.

[104] *Id.* at 15.

[105] *Id.*

create a loophole in the border search exception. Irving appealed the District Court's decision to the Second Circuit, which affirmed the District Court's decision.[106] However, the Second Circuit used a different line of logic and refused to decide whether the border search of the diskettes and film was routine or non-routine and instead found that the agents had reasonable suspicion based on the totality of the circumstances.[107]

A short time after the *Irving* case, the Fourth Circuit would hear an appeal on a border search of electronic media in *United States v. Ickes*.[108] John Ickes, Jr. was returning to the U.S. from Canada and told the Customs inspector that he was coming from a vacation, while driving a van that the inspector believed appeared to contain everything that Ickes owned.[109] As a result, Ickes was referred for a secondary inspection, during which a videotape was discovered that contained extensive footage of a young ball boy working a tennis match.[110] This further piqued the secondary inspectors' interests and the continuing search revealed several photo albums containing nude and semi-nude prepubescent boys in provocative poses; as well as "approximately 75 disks containing additional child pornography," one of which contained Ickes sexually abusing children.[111] On appeal, Ickes attempted to convince

---

[106] United States v. Irving, 432 F.3d 401 (2nd Cir. 2005).

[107] *Id.*

[108] United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).

[109] *Id.* at 502.

[110] *Id.*

[111] *Id.* at 503.

the court that 19 U.S.C. 1581 did not permit a search of his computer and diskettes.[112] The court refused to follow this reasoning; first because Congress has clearly authorized the search power of Customs officials and second, because the statute covers cargo, and the court believed that the computer and diskettes, being items inside Ickes van, were clearly cargo.[113] Ickes also attempted to argue that the search was simply unconstitutional, another argument by which the court was unpersuaded.[114] The court returned to *Ramsey* and *Flores-Montano* and held that searches at the border without probable cause or warrant have an extensive history of being considered reasonable.[115] The court, therefore, affirmed Ickes' conviction.[116]

In the Third Circuit in 2007, *United States v. Linarez-Delgado* would involve a border search of electronic media.[117] During a secondary inspection conducted on Linarez-Delgado, a Customs officer viewed footage contained on a camcorder in Linarez-Delgado's possession, revealing a nickname for Linarez-Delgado and evidence that he was a member of a drug trafficking organization with an outstanding arrest

---

[112] *Id.*

[113] *Id.* at 503-505.

[114] *Id.* at 505.

[115] *Id.* at 505-507. Ickes also attempted to persuade the court to carve out a First Amendment exception for expressive materials. The court refused this as well on the basis of *Ramsey* and Supreme Court precedent in New York v. P.J. Video, 475 U.S. 868 (1986), where there was refusal to require a higher standard for warrant issuance for expressive materials. Therefore, it was unlikely that such an exception could be created for the border search doctrine.

[116] *Id.* at 508.

[117] United States v. Linarez-Delgado, 259 Fed. Appx. 506 (3rd Cir. 2007).

warrant.[118] Linarez-Delgado was later convicted of numerous drug offenses.[119] On appeal, he sought to suppress the viewing of the footage, arguing that it was not permissible under the Fourth Amendment, but the court disagreed, again relying on the long history of jurisprudence allowing routine searches and seizures at the border without a warrant.[120] Ultimately, the court held that the viewing of the videotape was permissible as a function of a reasonable border search.[121]

The following year, the Ninth Circuit would hear *United States v. Arnold,* which involved the search of the data on a laptop after Michael Arnold returned to the United States from the Philippines.[122] Arnold was selected for a secondary inspection at Los Angeles International Airport, during which a Customs officer asked Arnold to boot up his laptop.[123] The officer subsequently opened a few folders on the desktop that indicated they contained pictures and observed a few nude photos.[124] A further search eventually revealed images believed to be child pornography.[125] Arnold was eventually convicted of possessing child pornography but, on appeal, argued that the search of his laptop was conducted without reasonable suspicion, and that a higher level of suspicion

---

[118] *Id.* at 507.

[119] *Id.*

[120] *Id.* at 508.

[121] *Id.* The court relied, inter alia, on *United States v. Ickes.*

[122] United States v. Arnold, 523 F.3d 941 (9th Cir. 2008).

[123] *Id.* at 943.

[124] *Id.*

[125] *Id.*

was required because of the amount of data a laptop may contain as opposed to other types of containers.[126] The court directly addressed the question as "[w]e must decide whether customs officers at Los Angeles International Airport may examine the electronic contents of a passenger's laptop without reasonable suspicion."[127] The court began by indicating that it was clearly established that searches of containers at the border were reasonable and then analogized laptops to other closed containers that were not subject to the same privacy and dignity interests as the human body.[128] Further, the court found that there was nothing in case law to suggest that a search became "particularly offensive" or required more suspicion merely because there was more material to be searched.[129] Ultimately, the court ruled that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."[130]

In 2011, the Ninth Circuit would again hear a case related to the border search of a laptop in *United States v. Cotterman*.[131] Initially, a divided panel would find no

---

[126] *Id.*at 943-944.

[127] *Id.* at 942.

[128] *Id.* at 944-946. The court relied, inter alia, on *Flores-Montano* and *Montoya de Hernandez* in its discussion of the privacy interests. The court focused on the Supreme Courts view of the vehicle as only property and that property did not implicate the same "dignity and privacy" concerns as the types of intrusive searches that might be conducted on a person's body, *Flores-Montano* 541 U.S. at 152.

[129] *Id.* at 947. The court was referring here to *Flores-Montano* in which the Supreme Court again left open the question of when a border search might be considered unreasonable because of its being effected in a "particularly offensive" manner.

[130] *Id.* at 946.

[131] United States v. Cotterman, 637 F.3d 1068 (9th Cir. 2011).

additional suspicion was required under the facts of the case, but the case would be reheard by the court en banc in 2012.[132] *Cotterman* involved the forensic search of a laptop that was detained at the border when Howard Cotterman returned from Mexico through the Lukeville Port of Entry in Arizona.[133] Cotterman was referred for a secondary inspection due to a criminal history for being a sex offender and a record indicating he may be involved in child sex tourism. Officers inspected his electronic devices, during which several password protected files were found on a laptop.[134] Although Cotterman offered to open the files, responding ICE agents were concerned that he might alter or delete the files; therefore, the laptops were detained and transported to Tucson, Arizona for a forensic search.[135] The search, conducted over the coming days, revealed a number of pornographic images involving children; and, after being contacted for assistance with the laptop, Cotterman fled the country.[136] At issue for the court was whether the government, using its authority to search a laptop at the border "without reasonable suspicion," could transport that same laptop to another location for a forensic examination.[137] The court considered a number of factors in its en banc consideration, to include the amount of data that is on a given computer hard

[132] United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013). The court would come to a slightly different conclusion in the rehearing than in the initial case.

[133] *Id.* at 957.

[134] *Id.* at 957-958.

[135] *Id.* at 958. The investigative arm of the Department of Homeland Security, referred to as ICE here, is now Homeland Security Investigations (HSI).

[136] *Id.* at 958-959.

[137] *Id*. at 959-961.

drive,[138] the sensitive types of information that people keep on their devices,[139] and the fact that a forensic search is an "exhaustive exploratory search" into this data that is "more intrusive than with other forms of property."[140] Ultimately, the court determined that the forensic search of Cotterman's laptop required a showing of reasonable suspicion (which was met), and hence setting the rule of law in the Ninth Circuit to require a showing of reasonable suspicion for the forensic search of a laptop computer pursuant to a border inspection.[141]

In 2014, *United States v. Saboonchi,* a case involving the forensic search of two smartphones and a flash drive collected pursuant to a border search, was heard in the United States District Court for the District of Maryland.[142] The district judge in the case, while dismissing the motion to suppress filed by Saboonchi, decided to file an opinion indicating his reasoning in the case.[143] Saboonchi was under investigation for violation of export controls to Iran and, after returning through Buffalo from a trip abroad, he was detained by CBP to further this investigation.[144] His electronic devices were

---

[138] *Id.* at 964.

[139] *Id.* at 966. The court specifically touched on "financial records, confidential business records, medical records, and private emails." *Id.* at 964.

[140] *Id.*

[141] *Id.* at 968-970.

[142] United States v. Saboonchi, 990 F. Supp. 2d 536 (Dist. of Md. 2014).

[143] *Id.* at 539.

[144] *Id.* The specific reason for the investigation was that Saboonchi had shipped a cyclone separator to the United Arab Emirates via a company that had business dealings with another of similar focus in Iran. *Id.* at 542-543. Saboonchi had also falsely represented that the separator was to remain in the United States. *Id.* at 543.

detained with the intent to search, but Saboonchi was released after answering some questions.[145] The judge, in his opinion, looked at the *Cotterman* decision from the Ninth Circuit and agreed with the finding that a forensic search is a search of a different kind and degree, holding that it was permissible only with reasonable and articulable suspicion.[146] However the judge also found that although reasonable suspicion was required, it was also present and well grounded.[147] However, this opinion was part of a denied motion to suppress, and therefore it cannot serve as precedent.[148] What it does serve as, however, is anecdotal evidence of some of the logic and positions courts outside the Ninth Circuit are using when electronic border search cases come before them.

As discussed in this part of the paper, the jurisprudence regarding the forensic border searches of laptop computers or other electronic devices has evolved away slightly from receiving the judiciary's automatic stamp of approval, at least in the Ninth Circuit. Whether this decision might become a trend amongst the other circuits, or be made nationwide binding precedent by the Supreme Court remains to be seen. At present, however, the Ninth Circuit is the only circuit with binding case law requiring articulable reasonable suspicion to conduct a forensic search of a laptop that is encountered pursuant to a border search. The other circuits still permit these forensic searches absent any articulable suspicion.

---

[145] *Id.*

[146] *Id.* at 548.

[147] *Id.* at 571.

[148] *Id.*

B – CBP Policy on Electronic Media Searches

The CBP Policy on electronic media searches was amended in 2007 to allow for suspicionless searches of travelers' electronic devices.[149] Pursuant to significant public concern, the policy was made public in summer 2008, to better inform the public of how CBP may conduct searches of their electronic devices.[150] In the wake of *Arnold*, the policy was updated and reissued in August 2009; and, because it remains the current version available to the public, it is this version that will receive focus.[151] Further, because it has already been established here that the electronic searches are in accord with Fourth Amendment case law, this section will merely present the parts of the policy that cover items not already addressed.

In the early part of the policy, what defines electronic media is addressed and is noted as "any devices that may contain information."[152] The list is not exhaustive, but covers what most people would consider to be electronic devices, or items that those devices might use, such as a disk or tape. The section also includes an open ended provision in saying "any other communication or digital devices."[153] The policy requires

---

[149] Carolyn James, *Balancing Interests at the Border: Protecting Our Nation and Our Privacy in Border Searches of Electronic Devices,* 27 SANTA CLARA COMPUTER & HIGH TECHNOLOGY L.J. 219, 226 (Feb. 2011).

[150] *Id.*

[151] U.S. CUSTOMS AND BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION (2009). This directive superseded the "Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008) to the extent they pertain to electronic devices." § 10.

[152] *Id.* at § 3.2.

[153] *Id.*

that each electronic device search be documented and, where practical, that a supervisor be present for the length of the search.[154] Further, the person whose device is being searched should be permitted to be present, unless operationally impossible, but not necessarily permitted to view the search.[155] Both of these ideals appear aimed at protecting the privacy interests of the traveler while still permitting the law enforcement goal of the search to proceed.

Because sensitive or privileged material of various natures could be encountered during an electronic media search, the policy addresses the handling of that material as well.[156] This is important because attorneys and medical professionals are likely international travelers and may possess this data on their devices. The policy essentially requires that questions or concerns regarding this information, especially if it is suspected to be evidence of a crime, to be referred to the Chief Counsel office within CBP, who "will coordinate with the U.S. Attorney's Office as appropriate."[157]

Data and devices may be detained up to five days with possible extensions as approved by upper level managers depending on the length of the continuation.[158] Any

[154] *Id.* at § 5.1.3.

[155] *Id.* at § 5.1.4.

[156] *Id.* at § 5.2.1 and 5.2.2.

[157] *Id.* at § 5.2.1.

[158] *Id.* at § 5.3.1.

data that is copied, and later determined to be of no value must be destroyed within seven days of that finding.[159]

Because CBP enforces laws for a number of federal agencies, outside those revolving around immigration and customs, the policy addresses receiving subject matter assistance from other federal agencies.[160] It permits the transfer of the device or copies of the data to another agency upon a finding of reasonable suspicion, and further indicates that reasonable suspicion is automatically satisfied if the person is included on a terrorism watch list.[161] Technical assistance however, addressing issues such as encryption, requires no reasonable suspicion.[162]

Finally, when probable cause exists the device may be seized and the information retained.[163] Further, all information retention must involve privacy-act compliant systems and must be appropriately safeguarded.[164]

Summarily, this section has demonstrated that although CBP has the authority to search electronic devices, these searches are conducted in a professional and privacy minded fashion. This is an important point demonstrating that, as an agency, CBP is not wildly searching devices and exposing travelers' private information to others.

---

[159] *Id.* at § 5.3.1.2.

[160] *Id.* at § 5.3.2.

[161] *Id.* at § 5.3.2.3.

[162] *Id.* at § 5.3.2.2.

[163] *Id.* at § 5.4.1.1.

[164] *Id.* at § 5.4.1.5.

IV. The Call For a Suspicion Standard on Electronic Media Border Searches

In the first two major parts of this paper, the border search exception was traced back to its roots, and some of the case law history addressing the search of electronic media in the border context was examined. Given that this paper has established the current state of the law regarding border searches of electronic media, it is now time to examine some of the arguments that surround the call for an additional suspicion standard in order to perform the searches. These sources vary in what level of suspicion they desire in order to perform a border search of electronic media, with the vast majority calling for a reasonable suspicion standard, while others call for a one articulable fact standard,[165] and still others for a probable cause and warrant standard.[166] One author even goes so far as to argue that the border search authority should be abolished altogether.[167] Additionally, the arguments vary from author to author with some overlap (probably more a result of concurrence amongst multiple secondary authorities).

It is important to note that the particular level of suspicion desired is not as important as the actual reasoning that is used to justify it. By this point it should be

[165] Ari B. Fontecchio, *Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception That Swallows Your Laptop,* 31 CARDOZO L. REV. 262 (2009).

[166] Samia Hossain, *Electronic Device Searches at the Border: It's Simple, Get a Warrant*, AMERICAN CIVIL LIBERTIES UNION (2015), http://www.aclu.org/blog/free-future/electronic-device-searches-border-its-simple-get-warrant.

[167] Cameron W. Eubanks, *Laptops, Airports, and the Border: Expanding Technology and the Shrinking Fourth Amendment in United States v. Arnold,* 64 U. MIAMI L. REV. 1117, 1135 (April 2010). The author very clearly argues for the complete abandonment of the border search exception, arguing "any search founded on neither probable cause nor reasonable suspicion should not be constitutional."

relatively clear what the state of the law is and, therefore, any increase in the suspicion level required would demonstrate a departure from the jurisprudence on the topic. To that end, this section proceeds under the assumption that regardless of the level of suspicion desired, the argument demands a change in the law. In order to explore these arguments thoroughly, each of the major arguments advanced in the various authorities will be addressed individually and explored.

A – Data Does Not Need to Cross the Physical Border to Enter (Or Exit) the United States

One of the first arguments advanced by some who call for an additional suspicion standard is that data does not need to be transported across the physical border in order to make entry into the United States.[168] Rasha Alzahabi, relying on the facts from *United States v. Romm*, argues that a child pornographer, for example, could access the illicit images across the internet from anywhere in the world.[169] On its face, this is not a poorly founded argument, but it fails when one considers that the crime charged in *Romm* did not actually involve the images being sent or received across the internet; rather, the crime involved the possession of the images and they were initially detected by Canadian officials during a border inspection.[170] So the mere fact that the images

[168] 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).

[169] *Id.* Citing United States v. Romm, 455 F.3d 990 (9th Cir. 2006). *Romm* involved the denial of entry of a US Citizen to Canada for possessing child pornography. After he was denied entry to Canada, the United States was advised of what had been found on his computer and officers were awaiting his arrival by air.

[170] United States v. Romm, 455 F.3d 990 (9th Cir. 2006).

could have been accessed across the internet does not lend itself to an argument that because that is an option for the criminal (or terrorist), the border searches of electronic media should be abandoned or require additional suspicion. Making such an argument is similar to saying that because radar detectors exist, and they effectively help some speeders avoid a ticket, that police should stop running radar altogether.

Alzahabi, however, is not alone in making this argument. In 2011, law student Victoria Wilson made a similar argument.[171] She claimed that the government's interest in conducting electronic media searches is lower because the very same data contained by those devices could simply be sent across the internet.[172] Therefore this "dangerous data," as she labeled it, was not necessarily prevented from entering the United States through the execution of these electronic media searches.[173] Again, the argument fails when one stops to consider that just because something *could* happen does not mean that it *does* happen. In other words, just because the internet could be utilized as a transport medium does not mean that it is. The argument is a bit disingenuous and is akin to saying that if there is a chance that something will not be found, because it might have been permanently lost, why waste the time looking for it?

Moreover, it is not inconceivable to believe that a criminal, such as a child pornographer, or a terrorist, would avoid sending what they perceive to be sensitive and

---

[171] Victoria Wilson, *Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States from Bombs, Drugs, and the Pictures From Your Vacation*, 65 U. MIAMI L. REV. 999, 1018 (Spring 2011).

[172] *Id.*

[173] *Id.*

valuable data across the internet without knowing for sure that it will not be intercepted. The internet, by design, contains an extensive system of shared servers and computers, any one of which could be exploited to allow the interception of data.[174] This is potentially a risk that these individuals do not want to take. Even in the wake of the exposure of electronic surveillance by Edward Snowden, would a terrorist or criminal organization blindly send data across the net hoping that it safely reaches its intended recipient, and is not intercepted by government or a rival group, as opposed to sending it with a trusted courier with whom the organization is familiar? This is a difficult question to answer, primarily because designing this metric would be nearly impossible, but the logic is there. Again, just because a particular method can be utilized does not mean that it is; and given the ability to perform the border searches of electronic media, it seems more unreasonable to ignore that as a possible avenue of inspection during an encounter with a traveler just because the data may have been sent another way.

B – Unrestrained Laptop Searches Can Lead to Profiling

Another argument advanced by opponents to border searches of electronic media is that without some imposed restraint, electronic media searches are likely to lead to profiling.[175] The specific concern appears to stem from allowing individual officers to exercise discretion in whom they choose to search, going so far as to use the searches to harass difficult travelers.[176] This argument appears to pay no particular

---

[174] Rus Shuler, *How Does the Internet Work?,* STANFORD UNIVERSITY, https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm.

[175] James, *supra* note 149, at 240.

[176] *Id.*

attention to the fact that law enforcement officers are trained to detect behavior that is suspicious or outside the norm. The author, Carolyn James, did not specifically say what constitutes profiling, nor did she offer any definition.[177] This is dangerous, because the term "profiling" cannot be constrained solely to those classes which are considered protected, such as race or religion. Webster's Dictionary offers one definition of profiling as "the act of suspecting or targeting a person on the basis of observed characteristics or behavior."[178] Therefore, although the most negative possible definition of "profiling" might come to mind, such as the alleged targeting of racial or religious groups,[179] that does not mean that all profiling behavior falls into this class. To clarify, the process of building a behavioral and psychological portfolio of a person, such as a serial killer, is also known as profiling. Such a profile focuses on the observed characteristics, behavior, and history of a person in that context.

For example, what if a Customs officer simply decided that for the next hour he was going to choose to search every person who refused to make eye contact with him during the primary inspection? Or what if the person was *profiled* on the basis of nervous behaviors, such as a pulsing carotid artery and shaky hands? Or, perhaps the traveler is intentionally being difficult with the ultimate goal of frustrating the inspection to such a degree that the Customs officer gives up and releases the traveler (behavior

---

[177] *Id.*

[178] *Profiling,* Merriam-Webster Online, http://www.merriam-webster.com/dictionary/profiling (last visited Apr. 27, 2016).

[179] Scott J. Upright, *Suspicionless Border Seizures of Electronic Files: The Overextension of the Border Search Exception to the Fourth Amendment,* 51 WM. & MARY L. REV. 291, 319-320 (October 2009).

sometimes labeled by officers as contempt of cop). Would these be acceptable reasons to take an inspection further? Would these articulable facts constitute the reasonable suspicion that James seeks? And if they did not meet the threshold of reasonable suspicion, does that mean that the electronic devices would necessarily be off limits, while everything else was still subject to search?

Moreover, the problem with the profiling argument is; how is a fixed standard developed for such a dynamic environment? It does not matter whether one is on the street in the interior of the country, or passing through an airport or land border, the fluidity and the dynamics of the environment demand that officers be given the discretion to determine, based upon their perception, when something is not right and to follow up on that information as necessary to resolve the encounter. To legislate and apply a rigid and fixed standard to a dynamic environment is to essentially legislate a great deal of inaction, as the standard will necessarily need to be stringent enough to avoid sweeping too many individuals into its net, yet relaxed enough to not miss everyone. Given the dynamic environments in which law enforcement officers operate, this is an unworkable principle.

C – The Amount of Data Electronic Devices May Contain Leads to a More Intrusive Search

A third argument advanced is that never before has a device been capable of carrying so much information, much of it highly personal, across the international border.[180] The general reasoning is that because a laptop, or other electronic device, is

[180] Wilson, *supra* note 171, at 1019.

able to store so much more information than other types of items, additional protection should be required because the search of that device stands to reveal far more about a person than does a search of some other type of item, such as a suitcase. For example, after Saboonchi appealed his case to the Fourth Circuit, the ACLU wrote a brief as amicus curiae in his support.[181] In that brief, the ACLU cites that hard drives of today's laptops can hold the equivalent of 600 million pages of text, having storage capacities of up to a terabyte or more.[182] Further, the ACLU argued that not only is the type of information that may be contained on the devices "exceedingly sensitive," it is in some cases sufficient to allow authorities the ability to reconstruct a person's entire life.[183]

There is no reason to argue the point over storage capacity, as it is scientific in nature and quantitatively measurable. However, there is one important caveat that needs to be considered. Not only do travelers willingly leave the United States and, similarly, willingly return; but they have the ability to make a conscious choice as to what items they travel with. If those items are electronic in nature, and capable of storing an extensive amount of information, the traveler could choose to remove items from the device that he would not want viewed by a person who were to perform a search, or to avoid bringing the device at all.[184] Professor LaFave has stated that "the individual

[181] Brief for Appellant, United States v. Saboonchi, (4th Cir. 2015) (No. 15-4111).

[182] *Id.* at 10.

[183] *Id.* at 12-14.

[184] Of important note here is the fact that, as the *Cotterman* decision noted, forensic searches have the ability to go far deeper than most cursory type searches. However,

crossing a border is on notice that certain types of searches are likely to be made" and therefore "the individual traveler determines the time and place of the search by his own actions" and can limit "the nature and character of the effects which he brings with him."[185] Moreover, electronic devices are not the first items ever to be tasked with containing personal information. Victoria Wilson concedes that items such as journals, photo albums, address books, etc., have the ability to reveal personal information; and questions why data stored on an electronic device should receive enhanced privacy protection just by virtue of that fact.[186] However, she argues that those other physical items may also be able to conceal contraband such as weapons or drugs while data on a laptop is not able to do any such thing. This is quite simply false, as how can one argue that child pornography, terrorist plans, pirated software or movies, or other digitized information that constitutes evidence of a crime (such as photographs or fraudulent financial ledgers) are not contraband? Therefore, the mere fact that a device can contain an extensive amount of information does not suddenly lend itself to an argument that it be subject to additional protections just due to the volume of information it contains. It is quite likely that the vast majority of the information present is of little value to law enforcement and would be passed over without a second thought.

---

just because a laptop has a cursory search performed on it by an officer does not immediately mean that it will be sent for a forensic search.

[185] Abidor v. Napolitano, No. 10-CV-04059, (E. Dist. N.Y. Dec. 31, 2013). Judge Korman cited Professor LaFave's opinion in arguing that the border context is different from a domestic context. Professor Wayne LaFave is Professor Emeritus at the University of Illinois, College of Law.

[186] Wilson, *supra* note 171, at 1018.

Consider a recreational vehicle (RV) for example. Some people travel extensively in RV's and use their RV as either an extension of their home, or possibly even their actual residence. Because an RV has the capability of storing so much more than an average car, or a suitcase hand carried by a traveler, does that mean that it is subject to additional privacy protections when crossing the border solely because it may contain more items? Logically, the answer is no. Although not a case involving a border search, the Supreme Court upheld the warrantless search of an RV by a DEA agent under the automobile exception, after the agent established probable cause that drug transactions were taking place within.[187] The Court held that the RV, given that it was only parked in a lot and was readily mobile, was far more akin to an automobile than a home, and therefore it was not entitled to the same protections as a physical residence.[188] Following that line of logic, and the applicable border search exception which requires no suspicion, it is unreasonable to believe that a court would suddenly opine for a higher suspicion standard to search an RV at the border based solely on the volume of contents or its likeness to a home.

As another example as to why not only volume, but also type of contents, is irrelevant in the border context, consider a moving truck that has to cross an international border as part of an international move.[189] Nathan Sales addressed this, pointing out that many (if not all) of a person's possessions would be included in this

[187] California v. Carney, 471 U.S. 386 (1985).

[188] *Id.*

[189] Nathan Alexander Sales, *Run For the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1112 (2009).

move, yet the truck and all of its contents would still be subject to a suspicionless border search.[190] It is not inconceivable to believe that some of the very same items a traveler might carry on his laptop or electronic device, he might likewise have in paper form in a filing cabinet or desk, which may be included amongst those personal possessions.

Ultimately, the mere fact that technology has changed how we carry information and to what degree, is not in itself sufficient to constitute a need for a higher suspicion level before searching an electronic device at the border. To the person whose data is being searched, the search itself may feel more intrusive; but because the person made a voluntary choice to subject that data to the possibility of search, the search cannot in itself be considered more intrusive than a search of any other type of property.

D – Deleted and Hidden Files May Be Discovered In Addition to Files the Owner Does Not Know Are Present

Opponents of suspicionless electronic media searches at the border also attempt to argue that the suspicionless searches may turn up files that the owner of the computer does not know are present.[191] These might include deleted files, files that were placed on the computer by a program without the knowledge of the owner, or location type data, amongst other things.[192] Bret Rasner argues that, therefore, digital information is not the equivalent of printed pages which, once shredded or otherwise

---

[190] *Id.*

[191] Elizabeth Bowersox, *Up In the Air: A New Framework for Laptop Searches in International Airports,* 35 OKLA. CITY U. L. REV. 885, 901-902 (2010).

[192] Brief for Appellant at 14, United States v. Saboonchi, (4th Cir. 2015) (No. 15-4111).

destroyed, are gone forever.[193] He argues that because these pieces of data are "easily recoverable" and may be "deeply personal" or "embarrassing" they cannot be grouped into categories of items that are searchable because they are "devoid of any dignity or privacy interests."[194]

There are a couple of issues with the argument of deleted or unknown files. First, while it is absolutely true that most items deleted on a computer are simply lying dormant while the space is waiting to be reused, that does not mean that a particular item ceases to be evidence solely because the owner tried to delete it. From a law enforcement perspective, it is somewhat advantageous that electronic devices may retain this information in a hidden form. For example, assume that a person commits a murder using a firearm and then throws the firearm into a river. Does the firearm cease to be evidence usable against the felon just because he believes he disposed of it in the river? Should the police not attempt to collect the firearm from the river because it has been "deleted?" Opponents to the suspicionless searches of electronic media would have one believe that a grave injustice is being perpetrated upon someone who perhaps attempted to erase evidence of a crime, but was unsuccessful in doing so. Second, from a certain perspective, the owner or consignee of any particular piece of property that is being transited across the border is responsible for what it contains. While many hidden or unknown files are probably just innocuous items connected with a given piece of software, it is also possible that they may reveal information that is

---

[193] Bret E. Rasner, *International Travelers Beware: No Reasonable Suspicion Needed to Search Your Electronic Storage Devices at the Border,* 3 PHOENIX L. REV. 669, 697 (Summer 2010).

[194] *Id.* at 698.

evidence of criminal or nefarious activity. However, in that context, how is data any different than the alternative with physical, tangible items? To clarify, assume that a person brings a suitcase through Customs that he is transporting as a favor for a friend and the suitcase is found to contain narcotics. Is the traveler suddenly able to disclaim that piece of luggage solely because he argues that he did not know that there were narcotics inside? Essentially, this argument is a disingenuous effort to allow individuals to disclaim responsibility for items that could serve as evidence against them.

E – Laptop Searches Take Longer Than Other Searches (Extensive Detention)

Another argument advanced by opponents is that "computer searches require fewer people but more time."[195] The concern here would seem to be that perhaps a connecting flight could be missed, or a person would spend a lengthy amount of time in customs. However, the counter-argument here is simply that, until a person has cleared the customs process, he or she is not admitted to the United States. Flights can always be rescheduled, and a missed connection, however frustrating and disappointing, is always a possibility in air travel regardless of whether it is domestic or international. Arguing that the customs process should be modified or ignored to facilitate catching a connecting flight is foolish. Land border crossings may involve other implications, but again, arguing in any way that Customs should abandon its duty due to conduct due diligence in the face of pending travel arrangements is a weak position to hold.

Opponents also advance that, because of the nature of laptop computers, and presumably other electronic storage devices, it is more likely to be removed from the

[195] Nicole Kolinski, *United States v. Arnold: Legally Correct But Logistically Impractical*, 6 J. L. ECON. & POL'Y. 31, 50 (Fall 2009).

possession of the traveler and detained at the border.[196] While this facilitates the release of the traveler while the device is still being checked, opponents then argue that business travelers and others, who rely extensively on their computers, would be deprived of their "virtual offices."[197] While this could certainly be of concern to those who have legitimate business functions to address, it is likely rare that a legitimate business traveler, who is not under suspicion of some type of crime, will have his laptop physically detained at the border in his absence. Statistics can better demonstrate the anomalous occasion under which a laptop is searched, let alone detained. From October 1, 2008 to May 5, 2009, 1,947 electronic media searches were conducted with 696 of those "performed on laptops" and only "forty were in-depth searches."[198] While those statistics do not demonstrate how often a device was detained in the absence of the owner, they do demonstrate that as rare as the electronic searches are, it is probably even rarer that a device will be detained in the absence of the owner. Therefore, although there is the possibility that a traveler will be separated from his or her device, it is misguided to institute a sweeping mandate requiring more suspicion over less than 2000 searches in a seven month period, especially when one considers that approximately 1,000,000 people pass through United States ports of entry per day.[199]

---

[196] Sid Nadkarni, *"Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices,* 61 UCLA L. REV. 148, 153 (2013).

[197] Kolinski, *supra* note 195, at 51.

[198] Bowersox, *supra* note 191, at 901.

[199] *On a Typical Day in Fiscal Year 2015,* U.S. CUSTOMS AND BORDER PROTECTION, https://www.cbp.gov/newsroom/stats/typical-day-fy2015 (last visited May 6, 2016).

The simple answer to the issue is that a laptop, as a piece of property, is subject to search as is any other piece of property, and the length of time it takes to search a given traveler's property should not be used to determine what level of suspicion is required to conduct that search.

F – Untrained Searchers Could Destroy the Device (Destructive Searches)

This argument was made by one particular law student as another reason for restraining searches of electronic devices or "technological equipment."[200] Nicole Kolinski relies on the opinion from *Flores-Montano* in which the Supreme Court stated that a property search may move from routine to non-routine if it becomes destructive.[201] She further relies on the opinion of the Ninth Circuit in *Arnold* in which they determined that such destructive searches would require reasonable suspicion.[202] However, despite the fact that Kolinski raises this issue, she fails to provide any evidence that such destruction has occurred, or how it might occur.[203] Worse, she opines that a higher suspicion level would help to avoid the whole situation altogether.[204]

There are a couple of distinct issues with the argument over searches being potentially destructive. First, there is the question of what would constitute a destructive

[200] Kolinski, *supra* note 195, at 51.

[201] *Id.*

[202] *Id.*

[203] *Id.*

[204] *Id.* at 52.

search. Of course the typical damaged device comes to mind where it somehow ceases to function physically. Does the possible corruption of files also fall into the destructive category? Before one can argue that device searches may be destructive, one should also provide parameters on what might constitute that destruction. Second, how does a higher suspicion level remove the risk of destruction of the electronic device? Although it would perhaps lessen the number of devices that are searched, if the risk of destruction were present with no particularized suspicion, how is it suddenly lessened through the presence of some articulable suspicion factors?[205] Essentially, this is a smoke and mirrors argument with no real substance as it would seem that any officer tasked with undertaking the search of an electronic device would necessarily take the required steps to protect that device, in the event it possessed evidence, as any loss of evidence would weaken the case.

G – Searches May Implicate Confidentiality Issues Related to Source or Client Information

Opponents of suspicionless border electronic media searches also express concern that confidential or protected client information will be jeopardized. A recent case involving such an argument was *Abidor v. Napolitano*.[206] In *Abidor*, a twenty-six year old was stopped on an Amtrak train near the service port of Champlain, New York.[207] Due to some inconsistencies in his travel documents, he was referred for

[205] *See* note 197. Less than 2000 searches of electronics were conducted in a seven month period that closely followed the conclusion of the *Arnold* case.

[206] Abidor v. Napolitano, No. 10-CV-04059, (E. Dist. N.Y. Dec. 31, 2013).

[207] *Id.* at 7.

additional inspection, during which his laptop was inspected; revealing photographs of terrorist organizations.[208] Although Abidor claimed that the photos were part of his dissertation on a specific sect of the Muslim faith in Lebanon, the laptop was detained for further review.[209] Two civic groups elected to back Abidor, arguing that the detention of his laptop was problematic because the respective individuals they represent, international photographers and attorneys who travel abroad, could have the confidentiality of their data or the anonymity of their sources breached by the suspicionless electronic searches.[210] The judge was unmoved by the argument and specifically stated that the "plaintiffs must be drinking the Kool-Aid" if they believed that a higher suspicion standard would allow for the ability to offer a guarantee of confidentiality because the United States border is not the only border crossed during international travel.[211] This is an astute argument and absolutely true; regardless of what protections the United States offers, those protections are not necessarily reciprocated by other countries the traveler visits.

Further, as discussed above in the section addressing the electronic media search policy implemented by CBP, there are protections in place for data that appears to be confidential or sensitive in nature.[212] For example, if the data appears to be

---

[208] *Id.* at 7-8.

[209] *Id.* at 8.

[210] *Id.* at 9-10.

[211] *Id.* at 22.

[212] U.S. CUSTOMS AND BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049 § 5.2.1, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION (2009).

attorney-client privileged data, the agency's Office of Chief Counsel must be consulted for guidance.[213] Although it is true that these are only policies, it demonstrates that the agency has taken seriously claims over the sensitivity of this type of information, and has taken steps to prevent its misuse. Of important note is that this policy was issued in 2009, four years before the Abidor case. Also, one must consider that CBP, in its goal of facilitating trade, is responsible for maintaining the integrity of extensive amounts of data regarding importations and exportations. Consider the impact that would occur on companies if CBP were not sound in its resolve to afford sensitive types of data the security it deserves.

Additionally, if privacy implications regarding the data were present when the search could be conducted with no suspicion, how are they lessened by adopting a higher suspicion standard? The only possible mitigating effect would be if the officer were unable to articulate the suspicion necessary to conduct the search. If this were the case, the search would obviously not be conducted; but if the requisite suspicion level is met, the argument over the potential privacy impact of the search would be completely moot.

H – A Warrant is Required in the Interior of the Country, Why Not More at the Border?

This argument attempts to justify a higher suspicion standard through a rather simplistic logic. The argument is essentially that because a warrant is required to search electronic media in the interior of the United States, a higher suspicion standard

[213] *Id.*

should be required to search the same devices at the border.[214] This is relatively simple logic to break, however, because a warrant is required to search property in the interior of the country, absent an applicable exception; but a warrant is not required to search property crossing the international border. This paper established that fact in part II, while examining the history of the border search exception and the present statutory authorities. Similarly, as discussed in the introduction, reasonable suspicion is required to perform a *Terry* stop of an individual on the street; but as any international traveler can tell you, in one way or another, no suspicion is required to be stopped at an international border crossing because everyone is stopped to facilitate the presentation of their documents and the making of a customs declaration.

Some of this argument stems from a recent Supreme Court decision in *Riley v. California*.[215] In *Riley*, the defendant was stopped for a traffic infraction and subsequently arrested for weapons charges.[216] He was suspected of being a gang member and police officers at the scene, seeking information that would establish this fact, searched Riley's phone incident to arrest for additional information.[217] The Court found the search of the phone to be invalid, relying on some of the same logic as has been set forth in the above subsections (privacy and storage implications), and ordered

[214] James, *supra* note 149, at 220.

[215] *Riley v. California*, 573 U.S. ___ (2014). The official court reporter is not yet released, but the opinion requests the citation form noted.

[216] *Id.*

[217] *Id.*

that a warrant be obtained before electronic devices taken incident to arrest may be searched for information.[218]

The reason why reliance on the *Riley* decision is faulty should be rather clear. Relying on the decision is a bit like comparing apples to oranges because it attempts to take the rules from one specific context (the streets in the interior of the country) and apply them to a totally different context (ports of entry and the international border). Life experience has probably demonstrated to the reader that this mode of thinking is often unsuccessful, as any time the playing field changes substantially, the methodologies must likewise change substantially to be successful in the operating environment (for example, football cannot be played with a baseball bat). Taking a rule established for police officers working on the streets and attempting to apply it to the international border setting is trying to stretch logic a bit too far.

I – Summary

In this part, the paper introduced and discussed a number of the arguments advanced by opponents to suspicionless searches of electronic media. Although the authors and proponents of the arguments have varying goals on the required level of suspicion they seek to achieve, they share an ultimate theme of eliminating suspicionless electronic media searches. In the next part, arguments for retaining a lack of individualized suspicion will be introduced and discussed.

[218] *Id.*

V. Why a Suspicion Standard is Dangerous

Having assessed the arguments made by opponents to suspicionless border searches of electronic media, this paper now turns its focus to why the creation of a suspicion standard for these searches would be dangerous. There are a couple of distinct arguments that will be made in this section, however, the vast majority of the academic sources encountered presented arguments for the creation of a suspicion standard, not against it. To that end, these arguments will primarily be supported with logical reasoning. In the first part of this section, the arguments against creating a suspicion standard will be introduced and discussed and, in the second part, a couple of court cases will be examined through the lens of what the outcome may have been had a suspicion standard been present.

A – Arguments Against Creating a Suspicion Standard

The following section addresses four reasons why creating a suspicion standard is dangerous, and could subject the country to additional and unnecessary risk. The reader is reminded that because there are relatively few sources that concur with this viewpoint, most of these arguments will be based on logical reasoning.

I – Loophole in Search Effectiveness is Created

Of all the arguments that may be made against creating a suspicion standard for border searches of electronic media, quite possibly the most persuasive is that it would create a loophole significantly reducing the effectiveness of border searches. At the end of part II, this paper examined how prevalent technology has become in our lives. It stands to reason that with this increase in technology, people are replacing time honored methods of scheduling, writing, taking and carrying photographs, etc. with new

and modern technological methods and devices. Searching any of those items during a border search has never been an issue in the past,[219] so the question becomes why such items are entitled to greater protection because of the manner in which they are carried. Creating a suspicion standard that is applicable solely on the basis that information is carried in an electronic device is akin to creating an exception for those devices, and such a broad exception to anything is dangerous.

To clarify how sweeping such a decision might be, as well as how devastating the impact, assume that the item in question is instead a suitcase and that the mandate was that no blue suitcases could be searched at the border absent reasonable and articulable suspicion (or worse yet, a probable cause or warrant standard). As word of this new suspicion standard spread, one would quickly see an increase in the use of blue suitcases, with the general traveler justification being something as simple as not wanting to have their luggage searched. But, for those who were attempting to evade Customs, the justification would be somewhat more nefarious. With knowledge that the suitcase could not be searched absent the requisite level of suspicion, the criminal would put all of his contraband into a blue suitcase in the hope that the Customs officers would not be able to develop enough suspicion to search it, and thereby discover the contraband. A blue suitcase would become a consular pouch of sorts, insulated from examination solely because of what it is.

Given the hypothetical "blue suitcase," apply the same logic to electronic devices. Is it not more likely that, given a higher suspicion standard, what a criminal or terrorist

[219] Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091 (March 2009).

might have carried on paper or printed photographs before, he or she would now store digitally in an effort to evade an inspection and subsequent discovery of the items? Essentially, creating a suspicion standard to search electronic devices opens an exploitable loophole that lessens the effectiveness of border searches.[220] If one item is eligible to go unsearched, it is there that the evidence of the crime will be placed. Return for a moment to *Cotzhausen v. Nazro*, in which the court stated that it would effectively be pointless to require declarations from persons arriving in the United States and to search their items, if one could simply exploit the mails to enter items at will.[221]

Quite simply, it cannot be permitted for individuals to evade customs through the use of a specific methodology. The former Secretary of Homeland Security, Michael Chertoff, made this same point, stating "we cannot abandon our responsibility to inspect what enters the U.S. just because the information is on an electronic device. To do so would open a dangerous window for terrorists and criminals to exploit our borders in new and unacceptable ways."[222]

II – Developing Required Suspicion May Be Difficult in a Fast Paced Customs Environment

A second argument against creating a suspicion standard is that in a fast paced international travel environment, such as a port of entry, developing the requisite

---

[220] Patrick E. Corbett, *The Future of Digital Evidence Searches and Seizures: The Future of the Fourth Amendment in a Digital Evidence Context: Where Would the Supreme Court Draw the Electronic Line at the International Border?,* 81 MISS. L.J. 1263 (2012).

[221] *Cotzhausen,* 107 U.S. at 218.

[222] Michael Chertoff, *Searches are Legal, Essential,* USA TODAY, Jul. 16, 2008, at 10A.

suspicion necessary to conduct a thorough search may be very difficult. As Ari Fontecchio states, the customs area is a "protected environment where officers encounter strangers for the first time" and as such it can be "difficult for an agent to develop a reasonable suspicion or probable cause."[223] To clarify Fontecchio's statement one must consider that every single person who conducts legitimate international travel to the United States will pass through Customs and Border Protection. Therefore, not only is the customs area typically full of people, many tired and irritable incident to their travel, but many are transplants from other places. Often, people do not know what to expect from the customs process, which may generate stress, nervousness, and other body language that law enforcement typically uses to pick out individuals who are engaged in criminal activity. Further, the reader will recall that Judge Korman, in his opinion to the *Abidor v. Napolitano* case, cited Professor LaFave in stating that travelers determine the time and place of the search when they pass through Customs.[224] This necessarily indicates that the choice to cross the border, and therefore encounter law enforcement, is voluntary and thus there exists no pre-text to the customs encounter.

This is vastly different from other types of law enforcement, to include street policing, as officers almost always have a reason for the encounter when they approach an individual. A police officer, in contrast to a Customs officer, is able to observe behavior as compared to the surrounding community and his accumulated knowledge thereof. Additionally, details such as time and place, mode of travel, person known to

[223] Fontecchio, *supra* note 165, at 263.

[224] Abidor v. Napolitano, No. 10-CV-04059, (E. Dist. N.Y. Dec. 31, 2013).

the officer, resident or non-resident of the community in which encountered, behavior upon observing the officer, etc., become useful articulable facts to support a stop. Further, time is often on the side of street law enforcement as, for example, a police officer sitting in a parking lot across the street could observe numerous suspected hand to hand drug transactions before deciding to stop the potential dealer. Customs, on the other hand, necessarily has to process individuals as quickly as possible (due to connecting flights, general space limitations, etc.) and pick out the "needles" in the "haystack" that may be up to no good.

Considering the differences between interior law enforcement and border law enforcement, it should be clear how it may be difficult to develop the requisite suspicion necessary to support a border search of electronic media, if the requirements are changed. When considering that creating a suspicion standard may create a loophole, as discussed above, the inability to reach the required level of suspicion to justify a search simply solidifies the loophole as an exploitable avenue.

III – Suspicion Standard Creates a Defense Mechanism for Challenging Evidence

Another, and relatively self-explanatory reason for not applying a suspicion standard to border searches of electronic media (or any border search, for that matter), is that it creates a potential defense mechanism against any evidence that is discovered in the search. As anyone who has spent time around criminal law (whether law enforcement, defense, or prosecution) will tell you, the easiest way to get evidence thrown out in a criminal case is to demonstrate that the government action before the discovery of evidence was unconstitutional. Therefore, due to this prior illegality, any evidence discovered is inadmissible under a concept known as "fruit of the poisonous

tree."[225] For example, assume that articulable reasonable suspicion is required to conduct an electronic media search at the border. An officer, believing that he possesses sufficient articulable suspicion, searches a laptop and discovers evidence of a crime. Prior to trial, the defense argues in a suppression hearing that the officer did not possess this articulable suspicion and the court agrees. Consequently, the search is now a bad search and the evidence is lost. Because most cases hinge on the evidence possessed by the government, the case will probably be dismissed or flat out lost by jury decision.

One does not need to look far to find recent examples of defense attorneys attempting to use this method to challenge their clients' arrests. Some examples of this tactic being used, whether successfully or not, include *United States v. Sanchez*[226] and *United States v. Hill.*[227] Regardless of whether the technique is successful in achieving the desired effect, it is clearly a valid starting point for an attorney challenging an arrest.

It is quite logical that such a tactic would be applied to border searches of electronic media if they are subjected to a suspicion standard. While the standard is certainly workable on cases in the interior of the country, it seems illogical to potentially put national security at risk by requiring a suspicion standard to search mere property

[225] BLACK'S LAW DICTIONARY 327 (4th Pocket Ed, 2011).

[226] United States v. Sanchez, 2016 U.S. App. LEXIS 5392 (1st Cir. Mass. Mar. 23, 2016). Challenge involved defense alleging that officers did not have R.S. to stop Sanchez based upon information from a confidential informant.

[227] United States v. Hill, 2016 U.S. App. LEXIS 5073 (7th Cir. Ill. Mar. 21, 2016). Hill challenged that there wasn't sufficient suspicion to conduct a *Terry* stop on him while he was observed feeding currency, stained red by a bank robbery dye pack, into a casino machine and removing voucher slips.

before it is permitted to enter the United States. Unable to meet this standard, officers may miss crucial information that could prevent terrorist attacks, or stop criminals who are returning from abroad before they return to the streets of the United States.

IV - Suspicion Standard Breaks with History

A final argument against creating a suspicion standard, while relatively simple, is that it breaks from the long history and tradition established for border searches. As identified in part II, the border search authority derives from an original congressional act older than the Fourth Amendment itself. It should be quite obvious that in the late 1700's there were no cars, no planes, and no one crossing the border on foot as a pedestrian. The only mode of entry was by ship and Customs' power applied to it directly. However, as technology evolved, Customs' power needed to evolve as well. Over the long history of the border search exception, the automobile came to fruition, and then the airplane (and subsequently international flights). Ports of entry were established along the Canadian and Mexican borders and, in modern day, pedestrians cross at many of these locations.[228] Over the long history of jurisprudence established for the border search exception, the courts have never hesitated to apply the plenary customs power to people (regardless of mode of travel), to the conveyance itself, to the items within the conveyance, or travelers' luggage.[229]

---

[228] *See* https://bwt.cbp.gov for all of the ports in the United States, to include which ports have pedestrian crossings.

[229] Remember, of course, that certain searches (non-routine) of the person do require a higher level of suspicion. But the routine search customs power applies solely by virtue of the crossing being made. *See* note 70 and *Montoya de Hernandez.*

Therefore, regardless of the arguments made by the opponents above, to establish a higher suspicion level for electronic device searches breaks with over 225 years of history and jurisprudence, solely because of reasoning such as the amount of data a device may carry, or the length of time it may take to search.[230] Further, given the increased capacity of these devices, it seems dangerous to search less when there is more being carried. With a higher volume of items, concealing the one dangerous item simply becomes easier, and when the ability to inspect those items for contraband becomes further limited by a suspicion standard, the ability of Customs to protect the country is threatened. In short, technology has never modified the basic tenets of the border search exception, therefore, why should it now?

B – Cases and Hypothetical Situations

In this section, two different court cases will be examined and a logical assessment will be conducted of how the case might have played out if a suspicion standard to conduct an electronic media search were present.

United States v. Tsai

In *United States v. Tsai,*[231] Immigration and Naturalization Service inspectors intercepted two aliens at the Guam International Airport who were attempting to travel to Hawaii on fraudulent passports. During the search of the arrestees' belongings, information was discovered which led the inspectors to believe that Hsi Huei Tsai was

[230] *See* part IV-C and E.

[231] United States v. Tsai, 282 F.3d 690 (9th Cir. 2002).

involved in assisting the aliens with their illegal travel to the United States.[232] After discovering that Tsai had already boarded the same flight to Hawaii, agents in Hawaii were contacted and asked to stop Tsai upon his arrival in Hawaii.[233] When Tsai was encountered in Hawaii, his bag and satchel were searched by INS and he was found to be in possession of a ticket jacket bearing the names of the individuals in the fraudulent passports.[234] Additional investigation revealed that Tsai was acting as an escort to the two individuals and he was later charged with "bringing unauthorized aliens to the United States for private financial gain."[235]

Tsai attempted to challenge his arrest by claiming that the border search of his belongings that revealed the ticket jacket was impermissible.[236] The court, however, disagreed and declared the search valid under the traditional principles of border searches.[237] Ultimately, Tsai's conviction was affirmed.[238]

In order to understand how this case might apply to a border search of electronic media, one must consider how many airline tickets are now issued electronically. Depending on the airline, one might even be able to use their smartphone as an

---

[232] *Id.* at 693.

[233] *Id.*

[234] *Id.*

[235] *Id.* at 694.

[236] *Id.* at 695.

[237] *Id.*

[238] *Id.* at 698.

electronic boarding pass that can be scanned at the jetway prior to boarding the plane.[239] Now assume that the Tsai case had been more recent, and instead of having the printed ticket jacket in his possession, Tsai instead had evidence of tickets and their purchase contained inside his smartphone. The question becomes whether or not the inspector who stopped Tsai upon his arrival in Hawaii would have possessed enough suspicion to meet the requisite standard to conduct a border search of electronic media. If he had not, Tsai might have been released, free to continue his efforts to smuggle aliens into the United States. Clearly, despite opponents who argue that a border search of electronic media does not fit within the scope of Customs,[240] such a search is clearly within Customs' enforcement purview. Is it not the scope and goal of customs and immigration enforcement to prevent the entry of contraband or illegal aliens into the United States? That is most certainly the goal, as was established in earlier parts of this paper.

Although hypothetical and based on facts that are altered to fit modern times, this situation should demonstrate how, simply because technology has changed our lives, exempting it from a border search can significantly reduce the effectiveness of Customs in protecting the country.

---

[239] *Mobile Boarding Pass*, AMERICAN AIRLINES, https://www.aa.com/i18n/travelInformation/traveltools/mobile-boarding-pass.jsp (last visited May 15, 2016).

[240] Eubanks, *supra* note 167, at 1137.

United States v. Ickes

Earlier in this paper, the *United States v. Ickes*[241] case was addressed during a review of the case law regarding border searches of electronic media. At this point it is useful to return to this case as a hypothetical example of how an increased suspicion standard for the border search of electronic media would impact the ability of Customs to keep the country safe.

The facts of the case do not need to be revisited here but the reader will recall that Ickes was referred for a secondary inspection, during which an officer viewed a videotape that was inside of a video camera, and that video focused extensively on a young ball boy at a tennis match.[242] Because the officer found this strange he made the search more extensive and eventually discovered and seized a computer and disks that contained child pornography.[243]

Of course it should be clear, without question, that the border search revealing this contraband was a win, in that it resulted in the discovery and arrest of a child predator. However, the border search involved what would be considered by opponents to be a search of electronic media. Referring back to the facts of the case above, would the officer have had the requisite suspicion required to view the videotape inside the camera? That is a question that may be left open for debate. It is quite possible that the officer did not possess reasonable suspicion and, if such were required for the

[241] United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).

[242] *Id.* at 502.

[243] *Id.* at 503.

viewing of the videotape, disks, and computer, that all of the evidence against Ickes would have been lost in court.

But, take the case a step further, and consider for a moment that it was not child pornography on the videotape, disks, and computer, but instead it was surveillance of government buildings or schools, and electronic spreadsheets revealing the levels and types of security as well as the times when particular locations were most vulnerable. Perhaps such information would constitute evidence of a crime, and perhaps it would not. But, logically speaking, what it could do is put someone on the radar as a potential threat to national security. It could prompt a further investigation, which might reveal a nefarious terroristic plot against the United States, a church or mosque, a university, or some other place of significant effect. What if the requisite suspicion level were not met in that particular case, would it cost the government the ability to keep the country safe? What is important to remember here is that the argument is not to create a police state. Rather, the argument is that, despite the increase in technology, the government cannot abandon the necessity to conduct thorough searches at the border to prevent the entry of contraband, illegal travel, or to detect nefarious plots against the United States.

VI. Other Countries Border Search Laws

Through the first five parts, this paper has examined: the history of the border search exception as well as its judicial history, its modern day application and statutory authorization, the positions of opponents as related to border searches of electronic media, and reasons why altering the exception would be dangerous. One question, however, might remain in the reader's mind. How does our border search law compare

to the laws of other countries, with whom the United States is allied, and that are on a similar level of advancement with regard to technology and the rights of citizens? This section of the paper will examine that very thing, using the border search laws of the United Kingdom and Canada to conduct this examination.

A - United Kingdom Border Search Law

The United Kingdom's border search law is derived from the Terrorism Act of 2000, and may be found in Schedule 7 of that act, otherwise called "Port and Border Controls."[244] The power to stop, question, and detain applies to a person if he or she is found "at a port or in the border area" and the officer believes that said presence at the port is connected with travel into or out of Great Britain or Northern Ireland.[245] In section 7, "Searches," it is made clear that examining officers (constables, immigration, and customs officers) all have the authority to search ships, aircrafts, vehicles, and persons.[246] Further, "goods" may be examined to determine whether they "have been used in the commission, preparation, or instigation of acts of terrorism."[247] For the purposes of this law, goods are defined as "property of any description"[248] or "containers."[249] This would apparently include laptop computers, for which no distinction is made in the law. In fact, in 2013, a reporter wrote that his laptop computer

[244] Terrorism Act, 2000, c. 11, § 53, Schedule 7 – Port and Border Controls (U.K.)

[245] *Id.* at § 53-2 (2).

[246] *Id.* at § 53-7.

[247] *Id.* at § 53-9.

[248] *Id.* at § 53-9(3)(a).

[249] *Id.* at § 53-9(3)(b).

was subject to search while traveling through the United Kingdom and that it was even detained due to suspicious materials that could compromise the security of the United Kingdom.[250]

Simply restating the law means nothing without discussion, so what is the significance of the above? From an objective reading of the law, it would appear that any person, vehicle, or item, including computers and other electronic devices, that is believed to be entering or leaving the United Kingdom is subject to search for the purposes of preventing terrorism. This is not different from the United States border search authority. Perhaps, as this paper has demonstrated, the original reasoning behind the United States border search authority was different and involved the collection of appropriate duty. However, not only does it continue to serve this purpose, it furthers the mission of CBP in preventing terrorism and instruments of terror from entering the United States.[251]

Overall, it seems that the United Kingdom's law regarding border searches is similar in scope to that of the United States, and therefore, despite what opponents might argue, the United States is not taking the border search authority to a new extreme.

---

[250] *Outrageous Searches on UK Border or How to Avoid Having Your Laptop Seized by Airport Authorities if You Are Taken For a Terrorist*, SPUTNIKNEWS (Feb. 25, 2013 5:37 PM), http://sputniknews.com/voiceofrussia/2013_02_25/Outrageous-searches-on-UK-border-or-how-to-avoid-having-your-laptop-seized-by-airport-authorities-if-you-are-taken-for-a-terrorist/.

[251] *About CBP,* CBP.GOV, https://www.cbp.gov/about (last visited May 18, 2016).

B - Canada Border Search Law and Legal Case

In Canada, the border search authority falls under the Canada Customs Act, Part IV – Enforcement.[252] The section of that act that covers the examination of goods may be found in Section 99, and states that an officer may examine any imported goods and "cause to be opened any package or container of imported goods."[253] Further, any goods that are possessed by a person inside of or leaving the "customs controlled area" are subject to search and a person may have their baggage, packages, or containers searched "if the officer suspects on reasonable grounds" that an "Act of Parliament" that is enforced by the officer is being violated by the goods.[254] Again, the law makes no distinction between a laptop computer or other electronic device, and packages, baggage, or containers.

Regarding electronic media searches, a challenge was made in 2008 over whether Canadian Customs officials had the right to search a laptop computer under the auspices of a container search. The challenge was specifically whether "a computer is a good like any other" and therefore subject to normal search at the border or was a "good like no other" and therefore could not be searched absent "a reasonable suspicion of contraband."[255] In making its decision, the court looked not only at Canadian case law but also at case law from the United States.[256] The court relied

---

[252] Customs Act, R.S.C. 1985, c.1 (2nd Supp.) s. 99 (1) (Can.).

[253] *Id.*

[254] *Id.* at s. 99.3 (2).

[255] *R. v. Leask*, 2008 ONCJ 25 (Can.).

[256] *Id*. at 6-7 (page numbers omitted).

heavily on *Flores-Montano* and found that booting up a computer and tapping on a few keys or using the device's search function was a "prosaically routine search in the context of a border search."[257] Further, a computer cannot be construed as an extension of the mind and searching it does not cause "fear and apprehension in a reasonable person."[258] Ultimately, the judge found that the search of the computer was a routine border search, effectively determining that a laptop computer falls within the same class of treatment as other property.[259]

Summarily, as of 2008, the country of Canada is approaching border searches in much the same way as the United States, including as they apply to searches of electronic media devices.

C – Summary

Although this section represents very brief glances at two other countries' border search laws, it should be clear that the United States is not the only developed country that conducts border searches of electronic media. The United States is not exploring uncharted territory by conducting these searches, regardless of how it may appear or what opponents may argue.

[257] *Id.* at 8 (page numbers omitted).

[258] *Id.* at 8 (page numbers omitted).

[259] *Id.* at 8-9 (page numbers omitted).

VII. Conclusion

This paper has traveled from the roots of the border search exception in the United States, through the jurisprudence that has affirmed and defined it, and examined the present day statutory authorities that authorize it. Further, this paper has examined border searches as they apply to electronic media devices, the arguments that opponents advance against such searches (and the reasons why those arguments are void), and why treating electronic media searches differently than other searches of property would be a dangerous proposition. Finally, this paper took a quick look at two other countries that are on a plane similar to the United States in terms of technology and legal position, and found that they are not dissimilar from the United States in regard to border searches, to include those of electronic media.

However, no examination of this topic would be complete without some basic recommendations, or to rehash what this paper advocates. If it has not been clear from the theme of this paper, it is necessary to maintain the border search exception in its present condition, with no further modifications. *United States v. Cotterman* has somewhat impacted the ability of border law enforcement in the Ninth Circuit to search electronic devices on a forensic level, although the ability to perform cursory searches of these devices has been left open.[260] Cases such as *Saboonchi* have further demonstrated that the courts are beginning to find a distinction between a forensic search of a device, and a mere cursory look.[261] However, it is vital that this trend not continue, regardless of reasoning, as the more electronic device searches are made

[260] United States v. Cotterman, 709 F.3d. 952 (9th Cir. 2013).

[261] United States v. Saboonchi, 990 F. Supp. 2d 536 (Dist. of Md. 2014).

distinctive from other types of searches, the more quickly individuals and organizations with nefarious intentions will shift to capitalizing on that distinction to skirt law enforcement at the border. Ideally, the Supreme Court will step in and return the United States to the roots of the border search exception, finding no distinction between electronic devices and their data, and other types of property. It should be clear that border law enforcement was established not only to support the country financially through duties, but to prevent the entry of unwanted individuals and items, which includes data of concern. Therefore, permitting a loophole to skirt such enforcement could essentially make the entire operation pointless.[262] Ultimately, the goal of this paper was to convince the reader how important it is that the United States maintain its historical border search authority roots, even as they apply to modern technology and situations.

It is also important to cover what this paper does not advocate. This paper does not advocate applying any of the principles of border searches to a context outside of the border or functional equivalent of the border (airports). This paper does not advocate for the suspicionless searches of persons or electronic devices in the interior of the United States. Further, this paper does not advocate modification of any other longstanding principles regarding searches and seizures as they apply in the interior of the country. Finally, this examination and discussion was not any kind of comment on the exchange of personal liberties for an increased measure of security. Rather, it simply argued against dismantling a longstanding government authority, likely to the

[262] Cotzhausen v. Nazro, 107 U.S. 215 (1883).

detriment of the security of the United States. Such a stance neither implicates the loss, nor the gain, of any personal liberties that Americans enjoy.

As any well-connected person can tell you, these are troubling times, at home and abroad. And, as technology facilitates communication and information transfer on a global scale as well as immense amounts of data storage, any small portion of which could be of concern, now is the not the time to cripple the ability of border law enforcement to examine what enters or leaves the United States on electronic devices. To do so may very well compromise the security of the United States, and that is simply unacceptable.