

## NOTE

### THE BORDER SEARCH EXCEPTION IN THE MODERN ERA: AN EXPLORATION OF TENSIONS BETWEEN CONGRESS, THE SUPREME COURT, AND THE CIRCUITS.

CHLOE MEADE

#### ABSTRACT

The Supreme Court has long held that the border is different when it comes to unwarranted searches and seizures. This is due to the government’s prevailing interest in “preventing the entry of unwanted persons and effects . . . at the international border.”<sup>1</sup> Circuit courts, however, are beginning to reconsider the scope of the border search exception when it comes to unwarranted forensic searches of electronic devices. The immense amount of data that can be extracted from advanced searches of cell phones and computers goes far beyond the information that could be uncovered through a physical search of what a traveler could carry. Following the Eleventh Circuit decision in *United States v. Touse*<sup>2</sup> which held that no reasonable suspicion is necessary to perform in-depth forensic searches of electronic devices at the border, a significant split emerged in the circuits. The Fourth and Ninth Circuits had previously held that some level of suspicion is necessary to justify forensic searches.<sup>3</sup>

Should the issue of the scope of the border search exception in the context of forensic searches of electronics reach the Supreme Court, the Court should hold that a warrant based on probable cause of a criminal act is required in order to perform a forensic examination of electronics. While this proposed solution may still provide imperfect privacy protection to non-citizens, a holding that falls short of a warrant requirement could have profoundly negative effects on non-citizen asylees and refugees seeking status in the United States.

---

<sup>1</sup> *United States v. Flores-Montano*, 541 U.S. 149, 149 (2004).

<sup>2</sup> *United States v. Touse*, 890 F.3d 1227, 1233 (11th Cir. 2018).

<sup>3</sup> *Compare* *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018) (requiring individualized suspicion), *and* *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (requiring reasonable suspicion), *with* *Touse*, 890 F.3d at 1233.

## CONTENTS

ABSTRACT.....	101
I. INTRODUCTION .....	103
<i>A. Forensic Electronic Searches</i> .....	104
<i>B. The Border Search Exception</i> .....	104
II. HISTORICAL JUSTIFICATIONS FOR THE BORDER SEARCH EXCEPTION .....	107
<i>A. Levying Duties on Goods and Intercepting Contraband</i> .....	108
<i>B. National Security Underpinnings of the Border Search Exception</i> .....	109
<i>C. Modern Institutions Administering Searches at the Border</i> .....	111
III. THE CIRCUIT COURT CONFLICT .....	113
<i>A. Riley v. California and the Border Search Exception</i> .....	115
<i>B. United States v. Cotterman and United States v. Kolsuz: Mandate         for Some Suspicion</i> .....	115
i. <i>United States v. Cotterman</i> .....	115
ii. <i>United States v. Kolsuz</i> .....	117
<i>C. United States v. Touset: No Reasonable Suspicion Necessary</i> .....	118
IV. A PROPOSED SOLUTION: REQUIRE A WARRANT SUPPORTED BY PROBABLE CAUSE OF CRIMINALITY TO PERFORM FORENSIC SEARCHES OF ELECTRONIC DEVICES AT THE BORDER.....	120
<i>A. The Supreme Court would likely hold that forensic searches at the         border are nonroutine but will not require a warrant</i> .....	121
<i>B. Policy Reasons for a Warrant Requirement to         Forensically Search Electronics at the Border</i> .....	123
V. EFFECTS OF WARRANT REQUIREMENT ON NON-U.S. CITIZENS .....	128
<i>A. A Warrant Requirement may not Fully Protect Non-Citizens at the         Border</i> .....	129
<i>B. Collateral Consequences of Forensic Searches for Non-U.S. Citizens</i> .....	130
i. <i>Prolonged Detention of Non-Citizens</i> .....	131
ii. <i>Harm to Asylum Applicants</i> .....	133
VI. CONCLUSION.....	134

## I. INTRODUCTION

On January 31, 2017, Mr. Bikkannavar (“Bikkannavar”), an optical engineer at The National Aeronautics and Space Administration’s (“NASA”) Jet Propulsion Laboratory flew into Houston, Texas from Santiago, Chile where he had been vacationing.<sup>4</sup> At passport control, Bikkannavar’s locked mobile phone was seized during a secondary inspection.<sup>5</sup> When a United States (“U.S.”) Customs and Border Protection (“CBP”) officer ordered Bikkannavar to disclose the password to his phone, he initially refused to do so, explaining that the phone belonged to his employer, NASA, and he was not supposed to disclose the password.<sup>6</sup> The CBP officer, however, insisted that they had the authority to search the device.<sup>7</sup> Bikkannavar, a Muslim American, asked the CBP officer why he was chosen for this secondary inspection but he never received an answer.<sup>8</sup>

A CBP officer then handed Bikkannavar a form entitled “Inspection of Electronic Devices” which stated:

“All persons, baggage, and merchandise . . . are subject to inspection, search and detention. . . . [Y]our electronic device(s) has been detained for further examination, which may include copying. . . . CBP may retain documents or information . . . . Collection of this information is mandatory . . . . Failure to provide information to assist CBP or ICE [U.S. Immigration and Customs Enforcement] in the copying of information from the electronic device may result in its detention and/or seizure.”<sup>9</sup>

Bikkannavar understood the form to mean that CBP had the legal right to search his phone and that refusal would result in CBP seizing his phone and copying the information contained therein.<sup>10</sup>

Bikkannavar ended up disclosing his phone’s password to CBP officials who took the phone into another room for thirty minutes.<sup>11</sup> The phone was returned to Bikkannavar and the CBP officer told him they had used “algorithms” to search the contents of the phone.<sup>12</sup> The use of algorithms to extract data from

---

<sup>4</sup> Amended Complaint at 5, 21, *Alasaad v. Duke*, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017).

<sup>5</sup> *Id.* at 21.

<sup>6</sup> *Id.* at 22; *see also* Lauren Grush, *A U.S.-born NASA scientist was detained at the border until he unlocked his phone*, THE VERGE (Feb. 12, 2017), <https://www.theverge.com/2017/2/12/14583124/nasa-sidd-bikkannavar-detained-cbp-phone-search-trump-travel-ban> [<https://perma.cc/DT49-9VFB>].

<sup>7</sup> Grush, *supra* note 6.

<sup>8</sup> *Id.*

<sup>9</sup> Amended Complaint, *supra* note 4, at 21-22.

<sup>10</sup> *Id.* at 22.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

Bikkannavar's phone indicates that CBP officers used one or more forensic tools to search the device.<sup>13</sup>

#### A. Forensic Electronic Searches

Bikkannavar's experience is not unique. The frequency of electronic device searches at the border more than doubled between fiscal year 2015 and 2016.<sup>14</sup> Even more alarming is the increased use of forensic tools that can uncover vast amounts of digital data that would otherwise be inaccessible through a manual electronic search.<sup>15</sup> A complaint filed in the Federal District Court of Massachusetts in *Alasaad v. McAleenan* outlines the intrusive nature of forensic searches:

In a forensic search, border officials use sophisticated tools, such as software programs or specialized equipment, to evaluate information contained on a device. Although there are different types of forensic searches, many of them begin with agents making a copy of some or all data contained on a device. Forensic tools can capture all active files, deleted files, files in allocated and unallocated storage space, metadata related to activities or transactions, password-protected or encrypted data, and log-in credentials and keys for cloud accounts . . . Officials then can analyze the data they have copied using powerful programs that read and sort the device's data even more efficiently than through manual searches.<sup>16</sup>

Digital forensics, or a forensic search is “the process of uncovering and interpreting electronic data.”<sup>17</sup> It is a powerful investigative technique that enables forensic examiners to review electronic data beyond the contents of a single hard drive within a laptop or hand-held device.<sup>18</sup> A forensic search extracts files, is capable of uncovering hundreds of pages worth of user data, and can even retrieve deleted material.<sup>19</sup>

#### B. The Border Search Exception

The Fourth Amendment to the U.S. Constitution protects the “right of the people to be secure in their persons, houses, papers, and effects, against

---

<sup>13</sup> *Id.* at 10.

<sup>14</sup> *Alasaad v. McAleenan (Formerly Alasaad v Duke)*, ACLU MASSACHUSETTS (Sept. 13, 2017), <https://www.aclum.org/en/cases/alasaad-v-duke> [<https://perma.cc/M7X9-JFUU>].

<sup>15</sup> See Amended Complaint, *supra* note 4, at 10 (explaining that a forensic search “expands the amount of private information officers could view during a manual search”).

<sup>16</sup> *Id.*

<sup>17</sup> David Tennant & Michael McCartney, *Forensic Examination of Digital Devices in Civil Litigation: The Legal, Ethical and Technical Traps*, 24 THE PROF. LAW. 13, 18 (2016).

<sup>18</sup> See *id.*

<sup>19</sup> *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013); see *United States v. Kolsuz*, 890 F.3d 133, 139 (4th Cir. 2018).

unreasonable searches and seizures.”<sup>20</sup> For a reasonable search, the Fourth Amendment generally requires whoever is conducting a search to obtain a warrant based on probable cause.<sup>21</sup> The “border search exception” allows U.S. customs and border officials to routinely perform unwarranted searches and seizures of persons and property at U.S. borders without probable cause or individualized suspicion.<sup>22</sup> In fact, government officials can conduct “‘routine’ searches based on no suspicion of wrongdoing whatsoever.”<sup>23</sup> Against the backdrop of the Supreme Court decision in *Riley v. California*,<sup>24</sup> circuit courts have begun to consider forensic searches’ constitutionality and the extent to which the border search exception may apply to invasive forensic searches.<sup>25</sup>

While there is no question that the border search exception is a historical doctrine that exempts customs and border officials from obtaining a warrant to search persons and their property at the border,<sup>26</sup> the circuits are split as to whether the doctrine extends to forensic searches of electronic devices.<sup>27</sup>

---

<sup>20</sup> U.S. CONST. amend. IV.

<sup>21</sup> *Katz v. United States*, 389 U.S. 347, 357 (1967) (“[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment - subject only to a few specifically established and well-delineated exceptions.”); see U.S. CONST. amend. IV; *California v. Acevedo*, 500 U.S. 565, 582 (1991) (Scalia, J., concurring) (explaining that rhetorically, by the 1960’s a warrant requirement was considered implicit in the Fourth Amendment’s requirement of reasonableness); see also *Chambers v. Maroney*, 399 U.S. 42, 51 (1970) (“[T]he Court has insisted upon probable cause as a minimum requirement for a reasonable search permitted by the Constitution. As a general rule, it has also required the judgment of a magistrate on the probable-cause issue and the issuance of a warrant before a search is made.”).

<sup>22</sup> *United States v. Ramsey*, 431 U.S. 606, 619 (1977) (affirming the “longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless ‘reasonable’...”); *Kolsuz*, 890 F.3d at 137; see also *United States v. Brignoni-Ponce*, 422 U.S. 873, 884 (1975) (“Except at the border and its functional equivalents, officers on roving patrol may stop vehicles only if they are aware of specific articulable facts, together with rational inferences from those facts, that reasonably warrant suspicion that the vehicles contain aliens who may be illegally in the country.”).

<sup>23</sup> KIM YULE, CONG. RESEARCH SERV., RL34404, BORDER SEARCHES OF LAPTOP COMPUTERS AND OTHER ELECTRONIC STORAGE DEVICES (2009).

<sup>24</sup> *Riley v. California*, 134 S. Ct. 2473, 2474 (2014).

<sup>25</sup> See, e.g., *United States v. Touse*, 890 F.3d 1227, 1233 (11th Cir. 2018); *Kolsuz*, 890 F.3d at 144; *United States v. Cotterman*, 709 F.3d 952, 952-53, 968 (9th Cir. 2013).

<sup>26</sup> See *Ramsey*, 431 U.S. at 617 (The “interpretation that border searches were not subject to the warrant provisions of the Fourth Amendment and were ‘reasonable’ within the meaning of that Amendment, has been faithfully adhered to by this Court.”); see also *Cotterman*, 709 F.3d at 963 (“Over the past 30-plus years, the Supreme Court has dealt with a handful of border cases in which it reaffirmed the border search exception....”).

<sup>27</sup> Compare *Kolsuz*, 890 F.3d at 144 (treating a border search of a phone as “non-routine” and “permissible only on a showing of individualized suspicion”), and *Cotterman*, 709 F.3d at 968 (requiring reasonable suspicion for search of a laptop at the border), with *Touse*, 890

Specifically, the circuits are divided over whether individualized or reasonable suspicion of criminality is necessary to perform an invasive and in-depth forensic search at the border.<sup>28</sup> The Fourth and Ninth Circuits have agreed that some suspicion of criminality is necessary to search an electronic device at the border, while the Eleventh Circuit held that no level of suspicion is necessary to justify a warrantless search.<sup>29</sup>

Many privacy advocates are encouraging the courts to require reasonable or individualized suspicion to perform a forensic search, but this Note argues that the Supreme Court should go further and require a warrant supported by probable cause of criminality before searching electronics seized at the border.<sup>30</sup> A warrant requirement is the only standard that ensures that searchers have sufficient probable cause to justify these invasive searches. A lesser standard allowing searchers themselves to evaluate whether there is reasonable or individualized suspicion would have the same effect as the Eleventh Circuit's holding that no suspicion is required to forensically examine electronics at the border.

Though the border search exception has existed in some form since the founding of the United States,<sup>31</sup> the Supreme Court has never endeavored to explicitly define its parameters. Instead, the scope of the exception has developed over time through statutory schemes and circuit court decisions.<sup>32</sup> Generally, the Supreme Court has maintained “[t]hat searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border . . . .”<sup>33</sup> The recent advent and proliferation of smart phones, laptops, and other

---

F.3d at 1233 (holding that the Fourth Amendment does not require any suspicion for a search of electronic devices at the border).

<sup>28</sup> Compare *Kolsuz*, 890 F.3d at 144 (requiring individualized suspicion), and *Cotterman*, 709 F.3d at 968 (requiring reasonable suspicion), with *Touset*, 890 F.3d at 1233 (holding that the Fourth Amendment does not require any suspicion).

<sup>29</sup> Compare *Kolsuz*, 890 F.3d at 144 (“[A] forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion.”), and *Cotterman* 709 F.3d at 968 (“[T]he forensic examination of Cotterman’s computer required a showing of reasonable suspicion, a modest requirement in light of the Fourth Amendment.”), with *Touset*, 890 F.3d at 1233 (“We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property.”).

<sup>30</sup> See, e.g., Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment Rights) at 40, *Alasaad v. Duke*, No. 1:17-cv-11730-DJC (D. Mass. filed Sept. 13, 2017) (In prayer for relief, plaintiffs request the Court declare that “searches of travelers’ electronic devices, absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws” is a violation of the Fourth Amendment).

<sup>31</sup> See *Ramsey*, 431 U.S. at 616-18; see also Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29.

<sup>32</sup> See *Touset*, 890 F.3d at 1234; *Kolsuz*, 890 F.3d at 137; *Cotterman* 709 F.3d at 968.

<sup>33</sup> *Ramsey*, 431 U.S. at 616.

electronic devices containing massive amounts of personal data has ushered in new challenges to the Constitutional limits of the border search exception.<sup>34</sup>

The first part of this Note provides the historical background against which the modern border search exception came into existence. Part two analyzes the circuit court cases that constitute the circuit split and predicts how the Supreme Court will rule if the issue of the border search exception in the context of forensic searches ever reaches the Supreme Court. The third part suggests a solution supported by policy arguments different from the holding the Court would likely reach; the Court should not sweep forensic searches of electronic devices into the border search exception and should instead require a warrant supported by probable cause. The final part considers the disparate impacts that even the proposed solution of a warrant requirement would have on non-citizens.

## II. HISTORICAL JUSTIFICATIONS FOR THE BORDER SEARCH EXCEPTION

In the modern world, the border search exception is not only seen as an exception deeply rooted in American historical jurisprudence, but is also inextricably linked with the belief that the exception is an important facet of a vital national security regime. The national security justifications for the border search exception, however, are relatively new and represent a departure from the intent of the Framers of the Constitution.

The underpinnings of the border search exception can be traced back to the first Federal Congress.<sup>35</sup> Throughout history, both Congress and the courts have justified and expanded the border search exception on the grounds that it is necessary to (1) tax goods entering the U.S.<sup>36</sup> (2) prevent the entry of contraband<sup>37</sup> and more recently to (3) protect U.S. national security interests.<sup>38</sup> What began as a mechanism for generating revenue and policing goods has in recent times been construed as a tool necessary to protect U.S. national security interests and prevent unwanted persons from entering the U.S.<sup>39</sup> The idea that

---

<sup>34</sup> See, e.g., *Touset*, 890 F.3d at 1234; *Kolsuz*, 890 F.3d at 137; *Cotterman* 709 F.3d at 968.

<sup>35</sup> See *Ramsey*, 431 U.S. at 616; see also Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29.

<sup>36</sup> See Act of July 31, 1789, ch. 5, § 21, 1 Stat. 29 (“An Act to regulate the Collection of the Duties imposed by law on the tonnage of ships or vessels, and on goods, wares and merchandises imported into the United States.”).

<sup>37</sup> See, e.g., *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (“Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband in this country.”).

<sup>38</sup> See, e.g., *Carroll v. United States*, 267 U.S. 132, 154 (1925) (“Travelers may be 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.”).

<sup>39</sup> See, e.g., Laura Nowell, *Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border*, 71 FED. COMM. L. J. 85, 100 (2018) (“Since the September 11<sup>th</sup> terrorist attacks, the government’s interest in monitoring the border has

the border search exception facilitates the policing of goods and contraband is profoundly different from the idea that it is necessary to screen people for criminals or terrorists. In the same way that American jurisprudence reflects a historical and political moment in time, the shift in the way the courts, the Legislature, and the people of the U.S. view the policing of the border informs the split between the circuits about the scope of the border search exception when applied to forensic searches of electronic devices.

#### *A. Levying Duties on Goods and Intercepting Contraband*

The first Congress, the same body that proposed the Bill of Rights, enacted the first customs statute, allowing customs and border officials the authority to board any ship suspected to contain concealed goods, wares, or merchandise.<sup>40</sup> When Congress first contemplated the Fourth Amendment in the context of the nation's borders, its primary concern was levying duties on goods imported into the U.S.<sup>41</sup> Guidance issued by the U.S. Department of the Treasury for Customs Officials in the late nineteenth and early twentieth centuries continued to frame border searches as primarily a means of locating and taxing goods coming into the U.S.<sup>42</sup>

In more recent years, the Supreme Court stated in dicta that the interception of "contraband" was contemplated by the founding fathers as a justification for the border search exception.<sup>43</sup> There is, however, little evidence that the first Congress considered contraband, in terms of illicit materials such as drugs or arms, as a primary goal of the border search exception. The prevention of illicit and harmful materials from entering the country emerged in large part when the U.S. banned alcohol from 1920 to 1933 during the prohibition era.<sup>44</sup> Whether

---

increasingly stemmed from the need to provide for national security and to thwart the growing threats of terrorism.").

<sup>40</sup> See *Ramsey*, 431 U.S. at 616; see also Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29.

<sup>41</sup> See Act of July 31, 1789, ch. 5, 1 Stat. 29.

<sup>42</sup> See U.S. Dept. of Treasury, Document No. 1406, Customs Regulations of the United States Prescribed for the Instruction and Guidance of Officers of Customs, Art. 360 (1892) ("All baggage of passengers from contiguous foreign territory shall be examined by an inspector at the port of first arrival, and, if dutiable goods are found contained therein, the amount of duties shall be assessed and collected."); see also U.S. Dept. of Treasury, Document No. 2492, Customs Regulations of the United States Prescribed for the Instruction and Guidance of Officers of Customs, Art. 1423 (1908).

<sup>43</sup> *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985); see also *Ramsey*, 431 U.S. at 619 (quoting *United States v. 12 200-Foot Reels of Super 8mm. Film*, 413 U.S. 123, 125 (1977)) ("The Constitution gives Congress broad, comprehensive powers '(t)o regulate Commerce with foreign Nations.' Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry.") (citation omitted).

<sup>44</sup> See Victoria Wilson, *Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders from Bombs, Drugs, and the Pictures from Your Vacation*, 65 UNIV. OF MIAMI L. REV. 999, 1003 (2011); see generally Brian Goff & Gary



Congress intended the border search exception to prevent the introduction of contraband into the U.S. in 1789 or not, the idea that border searches can and should be used to exclude illegal imports was first articulated a century ago.<sup>45</sup>

In 1952, the eighty-second U.S. Congress passed the Immigration and Nationality Act.<sup>46</sup> This act codified the border search exception in federal law.<sup>47</sup> The ability of border officials to conduct warrantless searches of individuals and their property remains a part of the Immigration and Nationality Act:

Any officer or employee of the Service authorized and designated under regulations prescribed by the Attorney General, whether individually or as one of a class, shall have power to conduct a search, *without warrant*, of the person, and of the personal effects in the possession of any person seeking admission to the United States, concerning whom such officer or employee may have reasonable cause to suspect that grounds exist for denial of admission to the United States under this chapter which would be disclosed by such search.<sup>48</sup>

The Immigration and Nationality Act of 1952 was ultimately modified significantly by the Immigration and Nationality Services Act of 1965.<sup>49</sup> However, the current language of 8 U.S.C. § 1357(c) is identical to the statute in the 1952 Immigration and Nationality Act and both clearly state that warrantless searches of persons and property are still permissible at the border.<sup>50</sup>

#### *B. National Security Underpinnings of the Border Search Exception*

Reflecting national consciousness following the September 11th terrorist attacks, the Supreme Court began to justify the border search exception using the government's national security interests during the 2000s.<sup>51</sup> The idea that border security furthers the government's national security interests is not entirely a product of the twenty-first century, but rather has its roots in racism.<sup>52</sup> Historically, attitudes towards different groups trying to immigrate to the U.S.

---

Anderson, *The Political Economy of Prohibition in the United States, 1919-1933*, 75 SOC. SCI. Q. 270, 271-273 (June 1994) (summarizing the historical development of prohibition and subsequent repeal in the U.S.).

<sup>45</sup> Wilson, *supra* note 44, at 1003.

<sup>46</sup> Immigration and Nationality Act, Pub. L. No. 414, ch. 477 (1952).

<sup>47</sup> *Id.* at Title II, ch. 9 § 287.

<sup>48</sup> 8 U.S.C. § 1357(c) (2006) (emphasis added).

<sup>49</sup> See generally Maddalena Marinari, *Divided and Conquered: Immigration Reform Advocates and the Passage of the 1952 Immigration and Nationality Act*, 35 J. OF AM. ETHNIC HIST. 9, 9-10 (2016).

<sup>50</sup> 8 U.S.C. § 1357(c) (2006); Immigration and Nationality Act of 1952, Pub. L. No. 414, ch. 477, Title II, ch. 9 § 287(c) (1952).

<sup>51</sup> See Laura Nowell, *Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border*, 71 FED. COMM. L. J. 85, 100 (2018).

<sup>52</sup> See Richard A. Boswell, *Racism and U.S. Immigration Law: Prospects for Reform After "9/11?"*, 7 J. GENDER, RACE & JUST. 315, 315-17 (2003).

have ranged from general hostility, experienced by many Europeans, such as the Irish in the 1800's,<sup>53</sup> to the adoption of overtly racist laws, like the Chinese Exclusion Acts.<sup>54</sup> While historians acknowledge that the Chinese Exclusion Acts were motivated largely by racial animus towards the Chinese-American community,<sup>55</sup> the acts nevertheless allowed the Supreme Court to consider the exclusion of persons attempting to enter its borders as necessary to keep the nation secure.<sup>56</sup> In 1925, the Supreme Court went a step further in *Carroll v. U.S.* and recognized that the ability of border agents to perform unwarranted searches at international borders was necessary to protect national security interests.<sup>57</sup> This represented a departure from the Supreme Court's prior rationale for the border search exception; the need to collect taxes on goods smuggled into the United States and to monitor contraband.<sup>58</sup> On its face, the idea that goods entering the country need to be policed is relatively innocuous, but the idea that *persons* entering the country need to be policed is rooted at least partially in racism.<sup>59</sup> When the impacts of the border search exception are viewed through a racial lens, it becomes evident that as the border search exception shifted from justifying the search of goods to the search of persons, it also broadened and got more teeth. The searching of persons is indicative of border officials looking for criminals and criminal activity, which leaves ample space for implicit bias and racism to shade decisions about which travelers are searched and why.

Throughout much of the twentieth century, the Supreme Court advanced an idea that has become a part of the modern border search exception: at the border, the individual expectation of privacy is less than the expectation of privacy within the U.S.,<sup>60</sup> and the interests of the U.S. must be balanced against the

---

<sup>53</sup> *Id.* at 318-19.

<sup>54</sup> *See, e.g.*, Act of May 4, 1882, ch. 126, § 1, 22 Stat. 58, 59 (1882).

<sup>55</sup> *See* Ernesto Hernandez-Lopez, *Global Migrations and Imagined Citizenship: Examples from Slavery, Chinese Exclusion, and When Questioning Birthright Citizenship*, 14 TEX. WESLEYAN L. REV. 255, 269 (2008) ("Chinese migration, despite being the result of domestic labor need and global movements, unfortunately faced nativist sentiment, racist discrimination, and reversal to the 1868 [Burlingame] treaty's invitations. These public and civil sentiments fed a series of measures from 1870 onward as part of the Chinese Exclusion process.").

<sup>56</sup> *See, e.g.*, *Fong Yue Ting v. United States*, 149 U.S. 698, 711 (1893) ("The right to exclude or to expel all aliens, or any class of aliens . . . [is] an inherent and inalienable right of every sovereign and independent nation, essential to its safety, its independence and its welfare . . .").

<sup>57</sup> *Carroll v. United States*, 267 U.S. 132, 154 (1925).

<sup>58</sup> *See, e.g.*, *United States v. Ramsey*, 431 U.S. 606, 616-617 (1977).

<sup>59</sup> *See* Boswell, *supra* note 52, at 317 ("From the early days of the new nation, the United States instituted far reaching . . . exclusionary measures to keep out foreigners. . . U.S. laws did not even consider African-Americans and others who were not 'free white persons' in the calculus of persons worthy of citizenship.").

<sup>60</sup> *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985).

interests of the individual.<sup>61</sup> In *U.S. v. Montoya De Hernandez*, the Court held that at international borders and their functional equivalents, “the Fourth Amendment balance of interests leans heavily to the Government.”<sup>62</sup> Though the Court did not expressly use the words “national security” it described government interests that are traditional national security concerns including; “protecting . . . [the] Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives.”<sup>63</sup>

In *U.S. v. Flores-Montano*, the Supreme Court cited the interest of preventing “unwanted persons” from entering the U.S. at the borders as a justification for these searches.<sup>64</sup> The *Flores-Montano* court also wrote that “the United States, as [a] sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity.”<sup>65</sup> The logic that searching travelers and their effects at the border is necessary to exclude persons and protect the territorial integrity of the United States provided a basis for Congress and the courts to consider national security concerns as a third, distinct justification for the border search exception.<sup>66</sup>

### C. Modern Institutions Administering Searches at the Border

The power to perform warrantless searches at the border is framed broadly and interpreted by various federal agencies as an exception that is necessary to promote national security interests.<sup>67</sup> Currently, the primary government agencies that are responsible for policing the borders and effectuating searches therein are CBP and ICE.<sup>68</sup> In March 2003, the Department of Homeland Security (“DHS”) was established in response to the September 11th terrorist

---

<sup>61</sup> See *id.* at 540 (“[T]he Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck more favorably to the Government at the border.”).

<sup>62</sup> *Id.* at 544; see *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973) (extending “functional equivalents” of a border to international airports and checkpoints outside of the actual border).

<sup>63</sup> *Montoya de Hernandez*, 473 U.S. at 544.

<sup>64</sup> *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).

<sup>65</sup> *Id.* at 153.

<sup>66</sup> See generally *id.* at 149.

<sup>67</sup> See, e.g., U.S. CUSTOMS AND BORDER PROT., *About CBP: Mission Statement*, U.S. DEPARTMENT OF HOMELAND SECURITY, <https://www.cbp.gov/about> [<https://perma.cc/6EKF-T4MV>]; U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, *Who We Are*, U.S. DEPT. OF HOMELAND SECURITY, <https://www.ice.gov/about> [<https://perma.cc/6XEY-NAXF>].

<sup>68</sup> See, e.g., U.S. DEPARTMENT OF HOMELAND SECURITY, *About DHS: History, Creation of the Department of Homeland Security*, U.S. DEPARTMENT OF HOMELAND SECURITY, <https://www.dhs.gov/creation-department-homeland-security> [<https://perma.cc/6D9D-JPRV>] (“[T]he Department of Homeland Security formally came into being as a stand-alone, Cabinet-level department to further coordinate and unify national homeland security efforts, opening its doors on March 1, 2003.”).

attacks.<sup>69</sup> The U.S. Customs Service was renamed Customs and Border Patrol<sup>70</sup> and was placed under the newly formed DHS.<sup>71</sup> The CBP's mission statement states that CBP exists "to safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel."<sup>72</sup>

CBP's mission statement and founding statute clearly address national security interests,<sup>73</sup> and the CBP website goes on to say that it "protect[s] the American people against terrorists and the instruments of terror."<sup>74</sup> ICE was established at the same time as CBP<sup>75</sup> and is the investigatory arm of DHS, operating to "protect the U.S. against threats to its national security and bring to justice those seeking to exploit U.S. customs and immigration laws worldwide."<sup>76</sup> Because ICE is responsible primarily for immigration enforcement within the U.S.,<sup>77</sup> this Note considers CBP as the primary government agency that administers searches at the border.

---

<sup>69</sup> President George W. Bush, *Proposal to Create the Department of Homeland Security*, U.S. DEPARTMENT OF HOMELAND SECURITY (June 2002), [https://www.dhs.gov/sites/default/files/publications/book\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/book_0.pdf) [<https://perma.cc/7KK8-FN2A>] ("After careful study of the current structure – coupled with experience gained since September 11 and new information we have learned about our enemies while fighting a war – the President concluded that our nation needs a more unified homeland security structure. In designing the new Department, the Administration considered a number of homeland security organizational proposals that have emerged from outside studies, commissions, and Members of Congress. The Department of Homeland Security *would make Americans safer . . .*").

<sup>70</sup> Reorganization Plan Modification for the Department of Homeland Security, Pub. L. No. 107-296, 116 Stat. 2135 (2002) ("(b) Rename the 'Customs Service' the 'Bureau of Customs and Border Protection'"); *see also* U.S. CUSTOMS AND BORDER PROTECTION, *About CBP: History-March 1, 2003 CBP is Born*, U.S. DEPT. OF HOMELAND SECURITY, <https://www.cbp.gov/about/history/march-1-2003-cbp-born> [<https://perma.cc/68KF-VN8Y>] ("On March 1, 2003, CBP was formed, and for the first time, border security responsibilities were placed together.").

<sup>71</sup> U.S. DEPT. OF HOMELAND SECURITY, *supra* note 68.

<sup>72</sup> U.S. CUSTOMS AND BORDER PROT., *supra* note 67.

<sup>73</sup> 6 U.S.C. § 211(c) (2017).

<sup>74</sup> U.S. CUSTOMS AND BORDER PROT., *supra* note 67.

<sup>75</sup> U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, *Celebrating the History of ICE*, U.S. DEPT. OF HOMELAND SECURITY, <https://www.ice.gov/features/history> [<https://perma.cc/9Q8C-HRD9>].

<sup>76</sup> U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, *Who We Are*, U.S. DEPT. OF HOMELAND SECURITY, <https://www.ice.gov/about> [<https://perma.cc/6XEY-NAXF>].

<sup>77</sup> *CBP and ICE: Does the Current Organizational Structure Best Serve U.S. Homeland Security Interests? Part II and III: Hearing before the Subcomm. on Mgmt., Integration, and Oversight of the Comm. on Homeland Sec. House of Representatives*, 109th Cong. 1 (2007) (statement of Rep. Mike Rogers, Chairman, Subcomm. on Mgmt., Integration, and Oversight of the Comm. on Homeland Sec.) ("U.S. Customs and Border Protection, referred to as CBP

## III. THE CIRCUIT COURT CONFLICT

Several circuits have considered the issue of whether the border search exception can be extended to in-depth and invasive forensic searches. The Ninth and Fourth Circuits have held that the border search exception extends to searches of electronic devices, but limited the scope of allowable forensic searches by applying a balancing test that weighs the government's interests against the privacy interests of the individual.<sup>78</sup> The Ninth Circuit in *U.S. v. Cotterman* held that a forensic search of a laptop at the border required "reasonable suspicion."<sup>79</sup> In *U.S. v. Kolsuz*, the Fourth Circuit largely followed the Ninth Circuit's decision in *Cotterman* but applied a slightly different standard, holding that agents at the border must have "some form of individualized suspicion" to conduct forensic searches.<sup>80</sup> In contrast, the Eleventh Circuit held that no suspicion is necessary to perform a forensic search at the border.<sup>81</sup> This difference in the scope of the border search exception represents a major split in the circuits that court watchers and commentators believe will likely end up in the Supreme Court.<sup>82</sup>

Reasonable suspicion is characterized as a "particularized and objective basis" for suspecting criminal conduct<sup>83</sup> and is thus a lesser standard of suspicion than probable cause.<sup>84</sup> Put simply, reasonable suspicion is a standard which is "more than a hunch but considerably below preponderance of the evidence,

---

. . . secures our borders and ports of entry; . . . U.S. Immigration and Customs enforcement, referred to as ICE . . . enforces our immigration and customs laws inside the United States.").

<sup>78</sup> See *United States v. Kolsuz*, 890 F.3d 133, 143 (4th Cir. 2018); *United States v. Cotterman*, 709 F.3d 952, 960 (9th Cir. 2013).

<sup>79</sup> *Cotterman*, 709 F.3d at 957.

<sup>80</sup> *Kolsuz*, 890 F.3d at 146.

<sup>81</sup> *United States v. Touset*, 890 F.3d 1227, 1234 (11th Cir. 2018).

<sup>82</sup> See, e.g., Grayson Clary, *Summary: Circuit Split on Device Searches at the Border in US v. Touset*, LAWFARE (May 30, 2018), <https://www.lawfareblog.com/summary-circuit-split-device-searches-border-us-v-touset> [<https://perma.cc/7YFL-QRG9>].

<sup>83</sup> See *Suspicion*, BLACK'S LAW DICTIONARY (11th ed. 2019) (Defining reasonable suspicion as "[a] particularized and objective basis, supported by specific and articulable facts, for suspecting a person of criminal activity."); See also *United States v. Arvizu*, 534 U.S. 266, 273 (2002) ("When discussing how reviewing courts should make reasonable-suspicion determinations, we have said repeatedly that they must look at the 'totality of the circumstances' of each case to see whether the detaining officer has a 'particularized and objective basis' for suspecting legal wrongdoing.").

<sup>84</sup> See *United States v. Sokolow*, 490 U.S. 1, 7 (1989) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)) (citations omitted) ("We have held that probable cause means 'a fair probability that contraband or evidence of a crime will be found,' and the level of suspicion required for a *Terry* stop is obviously less demanding than that for probable cause."); see also *Terry v. Ohio* 392 U.S. 1, 30-31 (1968) (recognizing that police may conduct a limited search and seizure with less than probable cause, including in situations "where a police officer observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot . . .").

which justifies an officer's investigative stop of an individual upon the articulable and particularized belief that criminal activity is afoot."<sup>85</sup> Probable cause, on the other hand requires a higher standard of suspicion.<sup>86</sup> According to the Supreme Court, the magistrate making a probable cause determination must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place."<sup>87</sup>

The courts have not expressly defined what constitutes a forensic search. The Fourth Circuit in *U.S. v. Kolsuz* described the forensic search that was the subject of the litigation as a search which, "extracts data from electronic devices and conduct[s] an advanced logical file system extraction."<sup>88</sup> The Ninth Circuit in *U.S. v. Cotterman* described computer forensic examination as "a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites."<sup>89</sup> The Eleventh Circuit in *U.S. v. Touse* did not define "forensic search," but contrasted a forensic search with a manual search which did not reveal illicit material, suggesting that a forensic search of an electronic device is more in-depth.<sup>90</sup> In each instance that the circuit courts consider a "forensic search," the search goes beyond a manual search of an electronic device and is able to reveal considerably more information than a standard "point-and-click" search of an electronic device.<sup>91</sup>

---

<sup>85</sup> AMERICAN LAW DIVISION, CONG. RESEARCH SERV. MEMORANDUM: PROBABLE CAUSE, REASONABLE SUSPICION, AND REASONABLENESS STANDARDS IN THE CONTEXT OF THE FOURTH AMENDMENT AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 1 (2006) (citations omitted).

<sup>86</sup> *Illinois v. Gates*, 462 U.S. 213, 236-37 (1983).

<sup>87</sup> *Id.* at 238.

<sup>88</sup> *United States v. Kolsuz*, 890 F.3d 133, 139 (4th Cir. 2018) ("the forensic examination did not reach data stored remotely – or 'in the cloud' – and was instead limited to data stored on the phone itself. Even so, the data extraction process ... yielded an 896-page report that included Kolsuz's personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates.").

<sup>89</sup> *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013).

<sup>90</sup> *United States v. Touse*, 890 F.3d 1227, 1230 (11th Cir. 2018) (An officer of the Customs and Border Protection Agency manually "inspected the iPhones and the camera, found no child pornography, and returned those devices to Touse. But the Agency detained the remaining electronic devices, and computer forensic analysts at the Department later searched them. Forensic searches revealed child pornography on the two laptops and the two external hard drives.").

<sup>91</sup> See Sean E. Goodison et. al., *Digital Evidence and the U.S. Criminal Justice System*, NAT'L INST. OF JUST. 1, 5 (2014), <https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf>.

*A. Riley v. California and the Border Search Exception*

It is important to view recent decisions about how the border search exception applies to electronic devices in light of the Supreme Court's landmark decision in *Riley v. California*,<sup>92</sup> which, in spite of its narrow holding, provided some guidance to lower courts on addressing privacy interests that are triggered by in-depth searches of electronic devices. In *Riley*, the Supreme Court unanimously held that when a cell phone is seized incident to arrest, a warrant is required in order to perform a search of the phone.<sup>93</sup> The *Riley* court recognized that the storage capacity of modern cell phones is so immense and the information contained therein so personal that a search of a cell phone or computer is fundamentally different from the search of other items that an individual may carry on their person.<sup>94</sup> The *Riley* court likened modern smart phones to "minicomputers" and held that for many Americans, cell phones contain "the privacies of life."<sup>95</sup> Though the holding in *Riley* is narrow and pertains only to warrantless searches and seizures of cell phones incident to arrest, the reasoning in *Riley* provides important insight into how the Supreme Court considers the personal nature of the data contained on electronic devices.<sup>96</sup> *Riley* also provided critical guidance to circuit courts considering forensic searches of electronics at the border, and both post-*Riley* circuit court decisions dealing with forensic searches of electronics at the border reference the *Riley* decision.<sup>97</sup>

*B. United States v. Cotterman and United States v. Kolsuz: Mandate for Some Suspicion**i. United States v. Cotterman*

In *U.S. v. Cotterman*, the Ninth Circuit considered the reasonableness of a forensic examination of a traveler's hard drive that was seized at the border.<sup>98</sup> Border officials searched Cotterman's laptop at a U.S.-Mexico border "in response to an alert based in part on a fifteen-year-old conviction for child molestation."<sup>99</sup> While the initial search at the border revealed no incriminating

---

<sup>92</sup> *Riley v. California*, 134 S. Ct. 2473, 2473 (2014).

<sup>93</sup> *Id.* at 2493-94.

<sup>94</sup> *Id.* at 2490 ("Allowing the police to scrutinize such records [contained in a cell phone] on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.").

<sup>95</sup> *Id.* at 2489, 2494-95.

<sup>96</sup> *Id.* at 2478-79 ("[C]ell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences . . . today many more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.").

<sup>97</sup> See, e.g., *United States v. Touset*, 890 F.3d 1227, 1234 (11th Cir. 2018); *United States v. Kolsuz*, 890 F.3d 133, 138 (4th Cir. 2018).

<sup>98</sup> *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013).

<sup>99</sup> *Id.* at 956.

material, Cotterman's laptop was nevertheless "shipped almost 170 miles away and subjected to a comprehensive forensic examination," which revealed the laptop contained images of child pornography.<sup>100</sup>

Citing the Supreme Court, the Ninth Circuit wrote that "the touchstone of the Fourth Amendment analysis remains reasonableness"<sup>101</sup> and held that a forensic examination of a computer seized at the border "required a showing of reasonable suspicion, a modest requirement in light of the Fourth Amendment."<sup>102</sup> The Ninth Circuit defined reasonable suspicion "as 'a particularized and objective basis for suspecting the particular person stopped of criminal activity.'"<sup>103</sup>

In its opinion, the Ninth Circuit turned to the Supreme Court's analysis in *Montoya de Hernandez* and *Flores-Montano*, which distinguished routine border searches from highly intrusive searches that go beyond the scope of a so-called "routine" customs search.<sup>104</sup> The Ninth Circuit recognized that a border search exception exists and that travelers entering the U.S. may be subject to *routine* searches without probable cause or reasonable suspicion. However, the Court found that the storage capacity of electronic devices and the nature of the content contained therein is so highly personal that it implicates "the Fourth Amendment's . . . guarantee of the people's right to be secure in their 'papers.'"<sup>105</sup> The discussion of the quantity and quality of the information contained within digital devices mirrors the reasoning that the Supreme Court adopted the following year in *Riley*<sup>106</sup> and stated that forensic analysis is "akin

---

<sup>100</sup> *Id.*

<sup>101</sup> *Id.* at 960 (citing *United States v. Montoya de Hernandez*, 473 U.S. 473, 538 (1985)).

<sup>102</sup> *Id.* at 968.

<sup>103</sup> *Id.* (quoting *United States v. Cortez*, 449 U.S. 411, 417-18 (1981)).

<sup>104</sup> *Id.* at 963 (first quoting *Montoya de Hernandez*, 473 U.S. at 540-41; then quoting *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004)) ("[T]he Court observed that it had 'not previously decided what level of suspicion would justify a seizure of an incoming traveler . . . other than a routine border search' and then went on to hold . . . that reasonable suspicion was required for 'the detention of a traveler at the border, beyond the scope of a routine customs search and inspection.' The Court's reference to 'routine border search' was parsed in a later case, *Flores-Montano*, where the court explained that 'the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person . . . [are] . . . dignity and privacy interests . . .')."

<sup>105</sup> *Id.* at 964, 967 ("International travelers certainly expect that their property will be searched at the border. What they do not expect is that, absent some particularized suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property for days . . .").

<sup>106</sup> *Compare Riley v. California*, 134 S. Ct. 2473, 2494-95 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)) (citation omitted) ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"), with *Cotterman* 709 F.3d at 964 ("The amount of private information carried by international travelers was traditionally circumscribed by the size of



to reading a diary line by line looking for mention of criminal activity- plus looking at everything the writer may have erased.”<sup>107</sup>

Furthermore, the Ninth Circuit, citing the Supreme Court in *Ramsey* recognized that government interests at the border, including the “long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country” must be balanced against individual privacy rights.<sup>108</sup> The Ninth Circuit agreed with Supreme Court dicta in *United States v. Montoya Hernandez*, which said that the balance at the border is “struck much more favorably to the Government.”<sup>109</sup> In the case of *Cotterman*, however, the forensic search was held to be so intrusive, and the invasion of dignity and privacy rights of the individual so significant, as to require reasonable suspicion, even at the border.<sup>110</sup>

ii. *United States v. Kolsuz*

In *United States v. Kolsuz*, “Kolsuz was detained at Washington Dulles International Airport while attempting to board a flight to Turkey because federal customs agents found firearms parts in his luggage.”<sup>111</sup> After Kolsuz was detained, his smartphone was subjected “to a month-long, off-site forensic analysis,” which yielded a “900-page report cataloguing the phone’s data.”<sup>112</sup> Kolsuz challenged the denial of his suppression motion, arguing that “the privacy interest in smartphone data is so weighty that even under the border exception, a forensic search of a phone requires more than reasonable suspicion” and should only be conducted with a warrant based on probable cause.<sup>113</sup>

The Fourth Circuit expressly framed the issue of forensic searches at the border in terms of routine and non-routine searches, acknowledging that the border search exception allows government agents to perform “routine” searches and seizures of persons and property without a warrant or any individualized suspicion.<sup>114</sup> However, the Fourth Circuit held that “nonroutine” searches at the border require an additional measure of suspicion,<sup>115</sup> and a

---

the traveler’s luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses of information.”).

<sup>107</sup> *Cotterman*, 709 F.3d at 962-63.

<sup>108</sup> *Id.* at 960 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

<sup>109</sup> *Id.* (quoting *Montoya de Hernandez*, 473 U.S. at 540).

<sup>110</sup> *Id.* at 962-64.

<sup>111</sup> *United States v. Kolsuz*, 890 F.3d 133, 136 (4th Cir. 2018).

<sup>112</sup> *Id.*

<sup>113</sup> *Id.* at 137.

<sup>114</sup> *Id.*

<sup>115</sup> Compare *Cotterman*, 709 F.3d at 957 (“[W]e consider the reasonableness of a computer search that began as a cursory review at the border but transformed into a forensic examination of Cotterman’s hard drive.”), with *Kolsuz*, 890 F.3d at 144 (“[W]e begin by considering the first premise of Kolsuz’s argument: that the forensic search of his cell-phone data qualifies as a nonroutine border search, requiring some level of particularized suspicion.”).

forensic examination of an electronic device is *not* a routine border search which therefore requires “some measure of individualized suspicion.”<sup>116</sup> Whether individualized suspicion is akin to “reasonable suspicion” or “probable cause,” the court declined to answer.<sup>117</sup> Despite citing *Cotterman*<sup>118</sup> and *Riley*, the Fourth Circuit punted on whether or not a warrant is required, holding merely that a forensic search of a digital phone is nonroutine and thus “requir[es] some form of individualized suspicion.”<sup>119</sup>

The Fourth Circuit found that “the scope of a warrant exception should be defined by its justifications” and acknowledged that in cases where searches are nonroutine, the Court may weigh the governmental interests at stake against the personal privacy interests of the individual.<sup>120</sup> The Fourth Circuit expanded that, “where the government interests underlying a Fourth Amendment exception are not implicated by a certain type of search, and where the individual’s privacy interests outweigh any ancillary governmental interests, the government must obtain a warrant based on probable cause.”<sup>121</sup> Government interests at the border include preventing the import or export of contraband by “those who would bring harm across the border . . . .”<sup>122</sup> In the case of *Kolsuz*, the government interest was the interception of illegal contraband at the border, and because there was a nexus between the government interest in preventing the export of arms and the search of the electronic device, the government interests outweighed *Kolsuz*’s privacy rights.<sup>123</sup>

### C. *United States v. Touset: No Reasonable Suspicion Necessary*

The Eleventh Circuit in *United States v. Touset* considered “whether the Fourth Amendment requires reasonable suspicion for a forensic search of an electronic device at the border.”<sup>124</sup> As Karl Touset was attempting to re-enter the U.S. after an international flight, border agents at the Atlanta Airport seized a number of his electronic devices because a “series of investigations by private

---

<sup>116</sup> *Kolsuz*, 890 F.3d at 137 (particularly in light of the Supreme Court’s decision in *Riley*, a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion).

<sup>117</sup> *Id.* (“[T]he forensic examination of *Kolsuz*’s phone must be considered a nonroutine border search, requiring some measure of individualized suspicion. What precisely that standard should be – whether reasonable suspicion is enough, as the district court concluded, or whether there must be a warrant based on probable cause, as *Kolsuz* suggests – is a question we need not resolve . . .”).

<sup>118</sup> *Id.* at 145 (noting that a forensic search can reveal “an unparalleled breadth of private information”).

<sup>119</sup> *Id.* at 146.

<sup>120</sup> *Id.* at 143.

<sup>121</sup> *Id.*

<sup>122</sup> *Id.* at 137.

<sup>123</sup> *Id.*

<sup>124</sup> *United States v. Touset*, 890 F.3d 1227, 1229 (11th Cir. 2018).

organizations and the government suggested that Karl Touset was involved with child pornography.”<sup>125</sup> Border officials seized two laptops, two external hard drives, and two tablets and, through forensic searches, the officials found child pornography on the laptops and hard drives.<sup>126</sup> Touset filed motions to suppress the evidence obtained from the forensic search of his electronic devices at the border, arguing that border patrol officials did not have reasonable suspicion to perform the search.<sup>127</sup>

The Eleventh Circuit held that the Fourth Amendment permits forensic searches of electronic devices at the border without any suspicion.<sup>128</sup> Relying in part on *Riley*'s narrow holding, the Eleventh Circuit dismissed the invasion of privacy argument, noting that *Riley* “does not apply to searches at the border.”<sup>129</sup> The court declined to follow dicta in *Riley*, which states that electronic devices are fundamentally different from other types of personal property, instead holding that electronic devices should not be treated differently.<sup>130</sup> The Eleventh Circuit went on to engage in a lengthy analysis of the differences between property and persons, reasoning that travelers are “free to leave any property they do not want searched—unlike their bodies—at home.”<sup>131</sup> The Eleventh Circuit justified its significant departure from the Fourth and Ninth Circuits by asserting that Congress, and not the courts, needs to adopt legislation to address the issue of forensic searches at the border if it feels the need to “provide greater protections than the Fourth Amendment requires.”<sup>132</sup>

The Eleventh Circuit also characterized government interests at the border as preventing unwanted persons and contraband from entering the country and protecting the “territorial integrity” of the United States.<sup>133</sup> It reasoned that because the government’s interests are heightened at the international border and the traveler’s privacy interests are lower, the weight of the government’s interests justifies suspicionless forensic searches in the context of border control.<sup>134</sup>

---

<sup>125</sup> *Id.* at 1230.

<sup>126</sup> *Id.*

<sup>127</sup> *Id.* at 1231.

<sup>128</sup> *Id.* at 1234.

<sup>129</sup> *Id.*

<sup>130</sup> Compare *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (“Allowing the police to scrutinize such records [contained in a cell phone] on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.”), with *Touset*, 890 F.3d at 1233 (“We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property.”).

<sup>131</sup> *Touset*, 890 F.3d at 1235.

<sup>132</sup> *Id.* at 1236.

<sup>133</sup> *Touset*, 890 F.3d at 1235. (quoting *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004)).

<sup>134</sup> *Id.*

IV. A PROPOSED SOLUTION: REQUIRE A WARRANT SUPPORTED BY PROBABLE CAUSE OF CRIMINALITY TO PERFORM FORENSIC SEARCHES OF ELECTRONIC DEVICES AT THE BORDER

If the issue of forensic searches of electronic devices at the border reaches the Supreme Court, the Court will likely adopt a framework that distinguishes between routine or basic border searches and nonroutine or advanced border searches, applying different standards of suspicion to each category.<sup>135</sup> This prediction is supported by the fact that shortly after argument in the *Kolsuz* case, the CBP distinguished “advanced” searches from routine searches and “adopted a policy that treats forensic searches of digital devices as *nonroutine* border searches . . . [that] may be conducted only with reasonable suspicion of activity that violates the customs laws or in cases raising national security concerns.”<sup>136</sup> According to the CBP directive, examples of a national security concern include “the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.”<sup>137</sup> While the CBP directive requires “reasonable suspicion” before performing an “advanced” search, the CBP fails to define what other “articulable” factors might contribute to a finding of reasonable suspicion.<sup>138</sup>

Based on Supreme Court precedent, if the Court categorizes searches as routine or nonroutine, it will most likely hold that in-depth forensic searches of electronic devices are nonroutine, and require some level of suspicion.<sup>139</sup> The primary question before the Supreme Court would therefore turn on the required level of suspicion necessary to justify an intrusive, “nonroutine” forensic search. The Supreme Court would then almost certainly include a balancing of government interests against the privacy interests of the individual to determine

---

<sup>135</sup> See *United States v. Montoya de Hernandez*, 473 U.S. 523, 538-541 (1985) (distinguishing “[r]outine searches of persons and effects of entrants [which] are not subject to any requirement of reasonable suspicion, probable cause, or warrant” from a nonroutine search, holding that nonroutine detention of a person to search her alimentary canal required reasonable suspicion.)

<sup>136</sup> *United States v. Kolsuz*, 890 F.3d 133, 146 (4th Cir. 2018) (citing U.S. CUSTOMS AND BORDER PROT., CBP Directive No. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (2018)).

<sup>137</sup> U.S. CUSTOMS AND BORDER PROT., CBP Directive No. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (2018).

<sup>138</sup> *Id.*

<sup>139</sup> See *United States v. Flores-Montano*, 541 U.S. 149, 149 (2004) (highly intrusive searches at the border might support a suspicion requirement); *Montoya de Hernandez*, 473 U.S. at 541 (holding that reasonable suspicion is necessary to detain and search a traveler suspected of alimentary canal smuggling.); *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973) (It is “without doubt” that the federal government has the power to effectuate “routine inspections and searches of individuals or conveyances seeking to cross our borders.”)

the level of suspicion necessary to justify a forensic search of electronic devices at the border.<sup>140</sup>

For the reasons outlined below, a standard that categorizes forensic searches of electronic devices as “advanced” or “nonroutine” and requires reasonable suspicion is preferable to an Eleventh Circuit-type standard that requires no level of suspicion to perform such a search at the border. The Supreme Court, however, should go a step further and require a warrant based on probable cause of criminality to perform such an advanced and invasive search of electronics at the border. This standard will better protect individuals from intrusive searches that violate the individual’s privacy interests. While the Court may be hesitant to require a warrant for these forensic searches and would rather defer to Congress and law enforcement’s ability to carry out national security objectives unchecked,<sup>141</sup> this Note argues that a warrant requirement is reasonable. A warrant requirement for a forensic search would ensure that in-depth, highly invasive searches remain rare, triggered only by probable cause of criminality as determined by a neutral magistrate.

*A. The Supreme Court would likely hold that forensic searches at the border are nonroutine but will not require a warrant.*

The Supreme Court would likely find that the in-depth nature of forensic searches of electronic devices is not routine, but would probably not require a warrant, instead deferring to the needs of law enforcement agencies in pursuing national security. This outcome is insufficient because it does not go far enough to protect the individual’s privacy interests.

If the question of a border search exception in the context of forensic searches of electronic devices reaches the Supreme Court, the Court would likely consider the CBP’s stated goals and mission, as well as their founding statutes and internal directives to identify the “government interest” that would be balanced against the interests of the individual.<sup>142</sup> The Supreme Court weighs government interests at the border heavily, citing the lack of “practical alternatives for policing the border” as a weighty interest that justifies intrusions of privacy.<sup>143</sup>

---

<sup>140</sup> *Riley v. California*, 134 S. Ct. 2473, 2496-97 (2014) (Alito, J., concurring in part and concurring with the judgment) (Reasoning that the proliferation of modern cell phones “calls for a new balancing of law enforcement and privacy interests.”); *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999) (Evaluating the reasonableness of a search by assessing, on the one hand, the degree to which it intrudes upon “an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.”); *Montoya de Hernandez*, 473 U.S. at 539 (“Balanced against the sovereign’s interests at the border are the Fourth Amendment rights of [the] respondent.”).

<sup>141</sup> *Kolsuz*, 890 F.3d at 153 (Wilkinson, J., concurring in the judgment) (In the context of border searches, “there is a longstanding historical practice . . . of deferring to the legislative and executive branches.”).

<sup>142</sup> *See Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc.* 467 U.S. 837, 848 (1984).

<sup>143</sup> *United States v. Brignon-Ponce*, 422 U.S. 873, 881 (1975).

Furthermore, under Chevron deference,<sup>144</sup> the Court would consider the CBP's interpretation of the statutes governing the border search exception, asking only whether the agency's interpretation of the statute "is based on a permissible construction of the statute."<sup>145</sup>

The CBP requires "reasonable" suspicion to perform what it terms an "advanced" (i.e. forensic) search.<sup>146</sup> In a CBP directive issued in January of 2018 describing its policy for the search of electronic devices at the border, the CBP categorizes searches as "basic" or "advanced."<sup>147</sup> The CBP defines an "advanced" search as one in which an officer "connects external equipment . . . to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."<sup>148</sup> This definition aligns with the forensic searches that occurred in *Kolsuz*, *Cotterman*, and *Touset*.<sup>149</sup> The CBP's internal policy about electronic searches at the border appears to be derived from *Kolsuz*, which held that "routine" searches at the border can be conducted without suspicion, while "nonroutine," or advanced, searches require some measure of individualized suspicion.<sup>150</sup>

According to the CBP memo, a "basic" search does not require reasonable suspicion,<sup>151</sup> while an advanced search requires "reasonable suspicion of activity in violation of the laws enforced or administered by CBP" or mere "supervisory approval" in instances involving a "national security concern."<sup>152</sup> The notion that searches which implicate a national security concern are effectively exempt from the reasonable suspicion requirement has been deemed a "huge loophole" that is so broad it will effectively "swallow" the rule.<sup>153</sup> This loophole demonstrates that the CBP, as an agency, believes the ability to quickly perform intrusive, "advanced" warrantless searches is paramount to promoting the national security interests of the United States.<sup>154</sup>

---

<sup>144</sup> See *Chevron*, 467 U.S. at 843.

<sup>145</sup> See *Chevron*, 467 U.S. at 843; 8 U.S.C. § 1357(c) (2006); 6 U.S.C. § 211 (2017); Aditya Bamzai, *The Origins of Judicial Deference to Executive Interpretation*, 126 YALE L.J. 908, 912 (2017) (Chevron deference "provides that a reviewing court must 'defer' to an administrative agency's reasonable interpretation of the organic statute that it administers.").

<sup>146</sup> U.S. CUSTOMS AND BORDER PROT., *supra* note 137.

<sup>147</sup> *Id.*

<sup>148</sup> *Id.*

<sup>149</sup> See generally *United States v. Touset*, 890 F.3d 1227, 1230 (11th Cir. 2018); *United States v. Kolsuz*, 890 F.3d 133, 139 (4th Cir. 2018); *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013).

<sup>150</sup> *Kolsuz*, 890 F.3d at 144.

<sup>151</sup> U.S. CUSTOMS AND BORDER PROT., *supra* note 137.

<sup>152</sup> *Id.*

<sup>153</sup> Sophia Cope & Arron Mackey, *New CBP Border Device Search Policy Still Permits Unconstitutional Searches*, ELECTRONIC FRONTIER FOUND. (Jan. 8, 2018), <https://www EFF.ORG/DEEPLINKS/2018/01/new-cbp-border-device-search-policy-still-permits-unconstitutional-searches> [<https://perma.cc/HCX5-XUMP>].

<sup>154</sup> U.S. CUSTOMS AND BORDER PROT., *supra* note 67.

Both the CBP and the Fourth Circuit require reasonable or individualized suspicion for forensic searches of electronic devices as part of “advanced” and “nonroutine” searches respectively.<sup>155</sup> This overlap suggests that the Supreme Court would likely categorize border searches in a similar manner and concede that forensic searches of electronic devices at the border are not, and should not be considered routine. Both the Fourth Circuit and the CBP require “reasonable” or “individualized suspicion” to effectuate a forensic search of electronics at the border, yet the CBP has been able to effectively lower the reasonable suspicion standard in cases where national security is implicated.<sup>156</sup>

The CBP’s ability to circumvent a reasonable suspicion standard shows that a more rigorous warrant requirement should be imposed on forensic searches of electronics to close this loophole. Given the cases where courts balance the needs of government (i.e. law enforcement) against the interests of the individual, the Supreme Court will almost certainly strive to ensure that any rule it articulates will allow administrative agencies the broad authority to execute searches at the border in the name of national security.<sup>157</sup> The inclination to make an exception for cases involving national security<sup>158</sup> is dangerous, and would further erode the Fourth Amendment in ways that expose travelers and individuals at the border to intrusions of privacy that should be unthinkable.

#### *B. Policy Reasons for a Warrant Requirement to Forensically Search Electronics at the Border*

The Supreme Court should require a warrant based on probable cause in order to conduct any forensic searches of electronic devices, regardless of whether border officials identify a national security risk. To obtain a search warrant, law enforcement officers must show there is probable cause to justify the proposed search.<sup>159</sup> According to the Supreme Court, the Fourth Amendment requires a “neutral and detached magistrate” to judge the “inferences” and evidence provided by law enforcement officers and issue warrants based on probable cause.<sup>160</sup>

---

<sup>155</sup> See *Kolsuz*, 890 F.3d at 144; U.S. CUSTOMS AND BORDER PROT., *supra* note 137.

<sup>156</sup> U.S. CUSTOMS AND BORDER PROT., *supra* note 137.

<sup>157</sup> *Wyoming v. Houghton*, 526 U.S. 295, 306 (1999) (In the case of the search of a passenger’s belongings in a car, the personal-privacy interest is ordinarily weak when compared to the needs of law enforcement.); *United States v. Montoya de Hernandez*, 473 U.S. 523, 541 (1985) (“[G]overnmental interests in stopping smuggling at the border are high indeed.”).

<sup>158</sup> *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (declining to extend the holding to “collection techniques involving foreign affairs or national security”).

<sup>159</sup> U.S. CONST. amend. V (“[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”).

<sup>160</sup> *Johnson v. United States*, 333 U.S. 10, 13-14 (1948).

Opponents to a warrant requirement will likely balk at this suggestion on many grounds, including the resources needed to apply for warrants. However, the reality is that an alternative, nebulous legal standard would allow the CBP to police itself. The CBP could adapt new legal standards in a way which suit its complex internal operating practices and objectives. Those internal operations do not appear to prioritize the privacy interests of the individual. The Supreme Court has addressed the problems inherent in allowing law enforcement officers to determine for themselves what types of searches do not violate the Fourth Amendment:

The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often-competitive enterprise of ferreting out crime.<sup>161</sup>

If the Supreme Court adopts a version of the CBP's vague policy for forensic electronic searches on cases involving national security, then CBP agents could have an incentive to invent, and subsequently report, justifications for forensic searches that comply with the law superficially. Those justifications and subsequent reports would constitute totally suspicionless forensic searches. Functionally, any standard below a warrant requirement could be abused.<sup>162</sup> The need for a bright line rule requiring CBP agents to obtain a warrant before forensically searching electronic devices at the border is therefore self-evident.

If CBP officers are required to prove that they have probable cause to a judge in order to obtain a warrant, (1) there will be a check on CBP's determination of what constitutes enough suspicion to warrant a forensic search and (2) the number of forensic searches at the border will likely decrease. While opponents may argue that any decrease in border searches will mean that the nation is less secure, if evidence of criminal activity exists, a warrant requirement would not be onerous. Requiring CBP agents to obtain a warrant will ensure that forensic searches at the border remain non-routine exceptions and do not become commonplace.

Admittedly, implementing a warrant requirement would necessarily require time and monetary resources. One of the main issues with the time required to obtain a warrant is that it could result in the prolonged detention of travelers awaiting the decision of a magistrate. Conceivably, a system could be implemented to allow travelers to leave their devices with CBP and await the decision of a magistrate from home—receiving their devices after a decision has been made. Nevertheless, both individual travelers and law enforcement would likely object to such a system. Travelers would argue that being deprived of their devices is fundamentally unreasonable while law enforcement would argue that

---

<sup>161</sup> *Id.*

<sup>162</sup> *See generally Montoya de Hernandez*, 473 U.S. at 538.



such a system frustrates law enforcement's ability to catch criminals at the border.

In the modern era, it is not impossible to envisage an electronic system whereby police officers could request and receive warrants within minutes using an online system.<sup>163</sup> For example, law enforcement officers in Marion County, Indiana adopted an electronic warrants system in 2017 which allows police officers to request warrants and receive a response from a magistrate or judge rapidly, in some instances in as little as half an hour.<sup>164</sup> The county then assigns digital warrant requests to judges who are issued tablets so that they can be "on-call" to receive and respond to warrant request from officers within minutes.<sup>165</sup> An electronic warrants system with on-call judges could also be a cost-effective method of administering a system that required warrants to perform forensic searches.

It should be noted that electronic warrant systems have been criticized and can produce troubling results.<sup>166</sup> For example, an investigation in Utah revealed that in a twelve-month period, 24 warrants were approved by judges in under a minute; more than half of the warrant requests were approved in under ten minutes and only 2% of warrant requests were denied.<sup>167</sup> Although these statistics are concerning, it is possible to imagine a system in which on-call magistrate judges at the border fairly adjudicate warrant requests before forensic searches can be carried out. Despite the costs and criticisms of a warrant requirement to forensically search electronic devices at the border, a warrant system that necessarily requires a neutral magistrate judge is preferable to allowing CBP to police itself and use a standard lower than probable cause to perform highly invasive searches.

Furthermore, it is dangerous to think about the issue of privacy rights at the border as something that only affects "criminals." The initial purpose of border searches<sup>168</sup> has been bastardized over time, as the border search exception is now

---

<sup>163</sup> See, e.g., Dermot McCauley, *Transforming the Search Warrant Process*, 69 SHERIFF & DEPUTY 78, 78-79 (2017); see also Jessica Miller & Aubrey Wieber, *Warrants approved in just minutes: Are Utah judges really reading them before signing off?*, THE SALT LAKE TRIBUNE (Jan. 14, 2018), <https://www.sltrib.com/news/2018/01/14/warrants-approved-in-just-minutes-are-utah-judges-really-reading-them-before-signing-off/> [<https://perma.cc/7REF-2RA5>]. (In a jurisdiction that uses e-warrants, "[p]olice officers write a description of their credentials and why they need access to whatever they want to search. Then they submit it digitally to the Utah Criminal Justice Information System. An on-call judge receives a text or email alert, and that can come at any hour of the day. The judge then reviews the warrant and makes a critical decision: Is there probable cause to believe a crime has been committed?").

<sup>164</sup> McCauley, *supra* note 163.

<sup>165</sup> *Id.*

<sup>166</sup> See Miller & Wieber, *supra* note 163.

<sup>167</sup> *Id.*

<sup>168</sup> See *United States v. Ramsey*, 431 U.S. 606, 616 (1977); see also Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43 (1789).

considered paramount to fighting crime.<sup>169</sup> The border search exception is currently ambiguous enough to allow CBP and border officials to forensically search the electronics of anyone entering or exiting the U.S. without a showing of probable cause or individualized suspicion.<sup>170</sup> It should also be noted that federal regulations grant CBP the authority to operate within 100 miles of any external U.S. boundary.<sup>171</sup> Roughly two thirds of the population of the United States live within 100 miles of an external boundary.<sup>172</sup> Though these statutes do not grant CBP the authority to perform warrantless and suspicionless searches of anyone within the “100-mile zone”, some scholars argue that this push into the interior is an attempt by CBP to expand the geographical boundaries of the border search exception.<sup>173</sup>

A Supreme Court holding that falls short of a warrant requirement for forensic searches could expose millions<sup>174</sup> of travelers a year to significant invasions of personal privacy that flow from unwarranted, suspicionless forensic searches of their electronic devices at ports of entry. It is impracticable to advocate that modern travelers must leave behind cell phones and other personal electronic devices when entering or exiting the United States in order to avoid intrusive, warrantless, and suspicionless searches upon entry and exit from the U.S.<sup>175</sup> The

---

<sup>169</sup> *United States v. Touset*, 890 F.3d 1227, 1235-36 (11th Cir. 2018) (the government has an interest in preventing the criminal dissemination and production of child pornography).

<sup>170</sup> *See Ramsey*, 431 U.S. at 616.

<sup>171</sup> 8 U.S.C. § 1357(a)(3) (2006) (“Any officer or employee of the Service authorized under regulations prescribed by the Attorney General shall have power without warrant . . . within a reasonable distance from any external boundary of the United States . . . .”); Field Officers; Powers and Duties 8 C.F.R. § 287.1 (a)(1) (2019) (“The term external boundary, as used in section 287 (a)(3) if the Act, means the land boundaries and the territorial sea of the United States extending 12 nautical miles from the baselines of the United States determined in accordance with international law.”); Field Officers; Powers and Duties, 8 C.F.R. § 287.1 (a)(2) (2019) (“The term reasonable distance, as used in section 287 (a)(3) of the Act, means within 100 air miles from any external boundary of the United States . . . .”).

<sup>172</sup> *The Constitution in the 100-Mile Border Zone*, ACLU (June 21, 2018), <https://www.aclu.org/other/constitution-100-mile-border-zone> [https://perma.cc/75HK-Y5FX].

<sup>173</sup> Hannah Robbins, *Holding the Line: Customs and Border Protection’s Expansion of the Border Search Exception and the Ensuing Destruction of Interior Fourth Amendment Rights*, 36 CARDOZO L. REV. 2247, 2271 (2014) (“CBP’s interior enforcement is an attempt to unconstitutionally expand the border search exception and must be curtailed.”).

<sup>174</sup> *See* U.S. CUSTOMS AND BORDER PROT., CBP TRADE AND TRAVEL FISCAL YEAR 2017 REPORT 1, 1 (2018) (“CBP officers processed more than 397.2 million travelers at air, land, and sea ports of entry in FY2017 . . . .”); *see also* UNITED STATES BUREAU OF TRANSPORTATION, 2017 TRAFFIC DATA FOR U.S. AIRLINES AND FOREIGN AIRLINES U.S. FLIGHTS (2018).

<sup>175</sup> *See Mobile Fact Sheet*, PEW RESEARCH CENTER (Feb. 5, 2018), <http://www.pewinternet.org/fact-sheet/mobile/> [https://perma.cc/69KN-6HZ6] (stating that 77% of U.S. adults own a smartphone); *see also* Ken Fox, *Passengers bring 2 or 3 electronic devices on flights*, LONELY PLANET (Feb. 16, 2016),

Fourth Circuit noted that “[p]ortable electronic devices are ubiquitous . . . and it is neither ‘realistic nor reasonable to expect the average traveler to leave his digital devices at home when travelling.’”<sup>176</sup> While the Eleventh Circuit holding in *Touset* effectively uses the border search exception to allow border agents to perform warrantless and suspicionless searches of traveler’s electronic devices with impunity, a standard of suspicion that carves out vast exceptions for national security would have a similar effect.

The Eleventh Circuit makes much of the heinous nature of possessing child pornography, and explains that “child pornography offenses overwhelmingly involve the use of electronic devices for the receipt, storage, and distribution of unlawful images.”<sup>177</sup> In both *United States v. Cotterman* and *United States v. Touset*, the forensic search performed at the border revealed that the respondents possessed child pornography.<sup>178</sup> While the importation of child pornography is illegal<sup>179</sup> and constitutes a heinous crime, if CBP officers have probable cause to believe that an entrant is in possession of child pornography, then surely they would almost always be able to obtain a warrant to forensically search a traveler’s electronic devices. The possession of child pornography cannot be likened to possession of a bomb or a weapon, which pose an immediate physical threat and require border officials to be able to act quickly and without a warrant. In any case, there are other well established Fourth Amendment exceptions like the exigent circumstances exception that would allow CBP officers to act quickly in the face of imminent danger.<sup>180</sup>

The Fourth Circuit contends that because child pornography can be classified as illegal contraband, border officials should be able to indiscriminately search

---

<https://www.lonelyplanet.com/news/2016/02/17/survey-air-passengers-bring-two-to-three-electronic-devices-on-flights/> [<https://perma.cc/TA3L-4MZQ>] (“New research has shown that 88% of people bring their smartphone with them when they are travelling for work . . . . The numbers bringing their smartphone drop- but only very slightly- on personal trips with 85% bringing their mobile . . .”).

<sup>176</sup> *United States v. Kolsuz*, 890 F.3d 133, 145 (4th Cir. 2018).

<sup>177</sup> *Touset*, 890 F.3d at 1236.

<sup>178</sup> *Id.* at 1230 (“Forensic searches revealed child pornography on the two laptops and the two external hard drives.”); *United States v. Cotterman*, 709 F.3d 952, 956 (9th Cir. 2013) (explaining that images of child pornography were found in Cotterman’s hard drive after a comprehensive forensic examination).

<sup>179</sup> 18 U.S.C. § 2260(b) (2008).

<sup>180</sup> *See Missouri v. Mcneely*, 569 U.S. 141, 149 (2013) (“A variety of circumstances may give rise to an exigency sufficient to justify a warrantless search, including law enforcement’s need to provide emergency assistance to an occupant of a home, engage in hot pursuit or a fleeing suspect, or enter a burning building to put out a fire and investigate its cause.”) (citations omitted); *see also United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir. 1984) (“[E]xigent circumstances . . . [are] those circumstances that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts.”).

electronics for child porn.<sup>181</sup> The court goes so far as to claim “if we were to require reasonable suspicion for searches of electronic devices, we would create special protection for the property most often used to store and disseminate child pornography.”<sup>182</sup> Justifying suspicionless forensic searches at the border on the grounds that officials *could* find child pornography is ludicrous and puts the privacy rights of the individual in peril.

The fact that a search occurs at the border should not mean that the Supreme Court can abandon the Fourth Amendment protections that individuals enjoy in the interior of the U.S. The Fourth Circuit’s argument surrounding child pornography also breaks down when one considers that in the age of the internet, distributors of contraband such as illicit images and content do not need to physically cross the border. If law enforcement agents cannot search the homes of distributors of illegal online content without probable cause and a warrant,<sup>183</sup> law enforcement should not be permitted to cast aside probable cause at the border to prevent the dissemination of illicit images.

There are a host of policy arguments that demonstrate why forensic searches of electronic devices at the border are intrusive, invasive, unavoidable for many people, and put the privacy interests of individuals at risk. What all of these arguments boil down to is relatively simple: if the Supreme Court is willing to classify forensic searches at the border as nonroutine or advanced, forensic searches should not be swept into the broader border search exception, but should instead require a warrant. In fact, the Court should require a warrant based on probable cause to perform a forensic search of an electronic device to ensure that these searches remain nonroutine.

#### V. EFFECTS OF WARRANT REQUIREMENT ON NON-U.S. CITIZENS

Given the current political climate, border issues are almost always considered in the broader context of immigration policy. For many, including CBP, immigration enforcement is viewed as necessary to protect the national security interests of the United States.<sup>184</sup> CBP thus serves a dual purpose of facilitating immigration enforcement and catching criminals at the border.<sup>185</sup>

---

<sup>181</sup> See *Touset*, 890 F.3d at 1233.

<sup>182</sup> *Id.* at 1235.

<sup>183</sup> *Payton v. New York*, 445 U.S. 573, 590 (1980) (“[T]he Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant.”).

<sup>184</sup> U.S. CUSTOMS AND BORDER PROT., *supra* note 67.

<sup>185</sup> Sophia Cope, *Law Enforcement Uses Border Search Exception as Fourth Amendment Loophole*, ELECTRONIC FRONTIER FOUND. (Dec. 8, 2016), <https://www.eff.org/deeplinks/2016/12/law-enforcement-uses-border-search-exception-fourth-amendment-loophole> [<https://perma.cc/P74Z-NUFV>] (The border search exception was created to enforce “immigration and customs laws, including ensuring that duties are paid on imported goods and that harmful people (e.g., terrorists) and harmful goods such as weapons, drugs, and infested agricultural products do not enter the country.”).

The concern with national security fuels the idea that the border search exception should be interpreted as broadly as possible. However, allowing for suspicionless forensic searches of electronics is fueled by nationalist, racist, xenophobic ideas about who deserves protection under the Constitution and who does not. The ironic fact of course, is that the border search exception applies to anyone who enters or exits the U.S. through a port of entry and affects both citizens and non-citizens.<sup>186</sup>

If the Supreme Court ruled on the border search exception in the context of forensic searches, it could give in to the historically racialized fears about terrorism, drug traffickers, and “bad hombres” that dominate the cable news cycle,<sup>187</sup> or it could choose to stop the systematic erosion of privacy rights initially conferred to individuals by the Fourth Amendment.<sup>188</sup>

This Note proposes a solution to the circuit split that would require CBP officers to obtain a warrant based on probable cause before performing forensic searches of electronic devices at the border. Due to the increasing criminalization of undocumented immigrants entering the U.S.,<sup>189</sup> the effects of a holding that falls short of a warrant requirement for forensic searches of electronic devices could have profound and unique effects on immigrants and refugees seeking shelter in the United States.

#### *A. A Warrant Requirement may not Fully Protect Non-Citizens at the Border*

In considering the ways in which a warrant requirement to forensically search electronic devices at the border would affect non-citizens, this analysis will first turn to a simple question: what exactly constitutes probable cause to search an electronic device? To obtain a warrant, law enforcement should have to show a nexus between the suspected crime and the need to search the electronic device. In other words, CBP should have to make a showing before a judge or magistrate that the forensic search of the electronic device is necessary to prove an element of the suspected crime. This would prevent the CBP from being able to obtain

---

<sup>186</sup> See U.S. CUSTOMS AND BORDER PROT., *supra* note 67.

<sup>187</sup> See, e.g., Matt Pearce, *Trump on immigration: ‘We have some bad hombres here, and we’re going to get them out’*, L.A. TIMES (Oct. 19, 2016), <https://www.latimes.com/nation/politics/trailguide/la-na-trailguide-third-presidential-trump-on-immigration-we-have-some-bad-1476927107-htmstory.html>; see also David Leonhardt & Ian Prasad Philbrick, *Donald Trump’s Racism: The Definitive List*, N.Y. TIMES (Jan. 15, 2018), <https://www.nytimes.com/interactive/2018/01/15/opinion/leonhardt-trump-racist.html>.

<sup>188</sup> U.S. CONST. amend. IV.

<sup>189</sup> Press Release, Department of Justice Office of Public Affairs, Attorney General Announces Zero-Tolerance Policy for Criminal Illegal Entry (Apr. 6, 2018), *available at* <https://www.justice.gov/opa/pr/attorney-general-announces-zero-tolerance-policy-criminal-illegal-entry> [<https://perma.cc/647Y-ZKT6>] (“[T]he Attorney General issued a memorandum to all federal prosecutors and directed them to prioritize the prosecution of certain criminal immigration offenses.”).

warrants when the suspected crime is entering the U.S. without inspection.<sup>190</sup> Entering the U.S. without permission should not warrant a search unless there is some other criminal activity underlying the entry.

If the Supreme Court fashions a probable cause standard modeled after *U.S. v. Ramsey*, which says a warrant can be obtained based on reasonable cause to suspect a violation of customs laws,<sup>191</sup> many individuals entering the U.S. through the Southern border without permission or inspection would be in violation of Immigration laws.<sup>192</sup> It is easy to imagine that warrants will be effortlessly obtained in a system where probable cause of violating an immigration law is the threshold inquiry. The CBP's "case" against aliens seeking entry to the U.S. would be easy to make in instances where migrants attempt to cross the border without inspection, or in cases where CBP officers suspect non-citizens of committing some type of fraud upon entry.<sup>193</sup>

Improper entry into the U.S. by an alien is a criminal misdemeanor punishable by no more than 6 months in prison.<sup>194</sup> Because of the criminalization of immigration violations, the Supreme Court will be left to grapple with questions like: should the mere fact that an individual has violated an immigration or customs law be the standard of probable cause to merit a forensic search of electronic devices at the border? Or, should some higher standard be applied, like probable cause to believe that an individual is suspected of a crime involving terrorism or drugs? One solution to this problem would be to distinguish between misdemeanors and felonies, with probable cause to suspect a misdemeanor not meriting a warrant to forensically search electronic devices.

The Supreme Court must ask itself; does a system that allows CBP officers to effortlessly obtain warrants upon suspicion of an immigration violation adequately protect the privacy rights of the individual? This question lends itself to another question: should the Supreme Court weigh the privacy concerns of non-U.S. citizens as heavily as it weighs the privacy interests of citizens? When one starts considering these tough questions, it becomes clear that maybe for non-citizens, even a warrant requirement to forensically search electronic devices does not go far enough.

### *B. Collateral Consequences of Forensic Searches for Non-U.S. Citizens*

A question that naturally flows from the discussion about what rises to the level of probable cause to forensically search electronic devices at the border is how information gathered from the search of an electronic device can be used against non-citizens or aliens. Could the information be transferred to U.S.

---

<sup>190</sup> See 8 U.S.C. § 1325(a) (1996).

<sup>191</sup> *United States v. Ramsey*, 431 U.S. 606, 607 (1977); see also Amended Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment Rights) at 40, *Alasaad v. Duke*, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017).

<sup>192</sup> 8 U.S.C. § 1325(a) (1996).

<sup>193</sup> 18 U.S.C. § 1546 (2002).

<sup>194</sup> 8 U.S.C. § 1325(a) (1996).

Customs and Immigration Services (“CIS”)<sup>195</sup> and used against applicants in asylum cases? Could the information be transferred to the Executive Office of Immigration Review (EOIR)?<sup>196</sup> Evidentiary rules are not the same in deportation hearings in the Immigration Court,<sup>197</sup> so there is ample space to use any of the information gathered in a forensic search against an alien in immigration court.

i. Prolonged Detention of Non-Citizens

A major potential collateral consequence that a warrant requirement could have for undocumented immigrants and arriving aliens would be the prolonged detention of aliens seeking entry to the U.S. while a warrant is obtained to forensically search their electronics. A warrant requirement necessarily takes time, which could require the detention of aliens at the border while CBP agents seek warrants from Federal Judges and Magistrates.<sup>198</sup> Under current regulations, CBP agents may “temporarily hold an individual at a CBP Port of Entry or Border Patrol Station” for “additional processing, including, for example, to determine identity and immigration status.”<sup>199</sup> Justice Brennan and Justice Marshall addressed the issue of detention to effectuate searches at the border in *U.S. v. Montoya de Hernandez*, stating that “involuntary

---

<sup>195</sup> See U.S. CITIZENSHIP AND IMMIGRATION SERVICES, *About Us: Mission Statement*, U.S. DEPT. OF HOMELAND SECURITY, <https://www.uscis.gov/aboutus> [<https://perma.cc/JN45-4SLF>] (“U.S. Citizenship and Immigration Services administers the nation’s lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.”).

<sup>196</sup> See Executive Office for Immigration Review, *About the Office: EOIR Mission* U.S. DEPT. OF JUSTICE, <https://www.justice.gov/eoir/about-office> [<https://perma.cc/Y2ML-2JRD>] (“The primary mission of the Executive Office for Immigration Review (EOIR) is to adjudicate immigration cases by fairly, expeditiously, and uniformly interpreting and administering the Nation’s immigration laws. Under delegated authority from the Attorney General, EOIC conducts immigration court proceedings, appellate reviews, and administrative hearings.”).

<sup>197</sup> See *Baliza v. INS*, 709 F.2d 1231, 1233 (9th Cir. 1983) (“Administrative proceedings are not . . . bound by strict rules of evidence.”); see also EOIR, IJ Benchbook, *Evidence Guide*, <https://www.justice.gov/eoir/page/file/988046/download> [<https://perma.cc/39TQ-QA8N>] (citing *Matter of Ponce-Hernandez*, 22 I&N 784 (BIA 1999); then citing *Matter of Toro*, 17 I&N Dec. 340 (BIA 1980)) (stating that relevance and fundamental fairness are the only bars to admissibility of evidence in deportation cases).

<sup>198</sup> 19 U.S.C. § 1595(a)(1) (1990) (Customs agents “may make application, under oath, to any justice of the peace, to any municipal, county, State, or Federal judge, or to any Federal magistrate judge, and shall thereupon be entitled to a warrant . . .”).

<sup>199</sup> U.S. CUSTOMS AND BORDER PROT., *Border Security: Immigration Action-For Individuals in CBP Custody*, U.S. DEPT. OF HOMELAND SECURITY, <https://www.cbp.gov/border-security/immigration-action> [<https://perma.cc/6KMQ-HVEJ>].

incommunicado detentions ‘for investigation’ are the hallmark of a police state, not a free society.”<sup>200</sup>

CBP operates twenty-four hours a day, and during the 2017 Fiscal Year, CBP encountered approximately 600 “inadmissible” individuals at ports of entry every day.<sup>201</sup> If CBP wanted to forensically search the electronic devices of even 10% of “inadmissible” individuals, and if those searches required a warrant, over the course of one year, the agency would have to seek approximately 21,900 warrants.<sup>202</sup> It is unclear whether CBP has the capacity to detain individuals while they attempt to obtain a warrant. It is possible that individuals detained by CBP for no other reason than their desire to search those individuals’ electronics could be transferred to ICE, which maintains a detention system that is overburdened and notoriously clumsy in record-keeping processes.<sup>203</sup> As this Note advocated in the previous section, the hope is that a warrant requirement to perform forensic searches of devices would drastically reduce the number of searches that are performed, and that law enforcement would seek warrants only in exceptional cases where there is legitimate cause to suspect a felonious crime.

The numerical burden of warrant requests would be spread across the hundreds of points of entry to the United States,<sup>204</sup> but would still represent a significant increase in the demand on judges and magistrates to hear warrant proceedings. Even if a thoughtful system were put in place and the number of magistrates at the border was increased or an electronic warrants system were adopted, a warrant requirement could still result in the detention of individuals.

Given the family separation cases that occurred in the Summer of 2018, there is an argument to be made that the detention of any alien at the border poses risks to that individual’s personal health and safety.<sup>205</sup> Multiple reports described

---

<sup>200</sup> *United States v. Montoya de Hernandez*, 473 U.S. 531, 550 (1985) (Brennan, J., dissenting).

<sup>201</sup> U.S. CUSTOMS AND BORDER PROT., *supra* note 67.

<sup>202</sup> *See id.*

<sup>203</sup> *See, e.g.*, Lisa Riordan Seville, Hannah Rappleye & Andrew W. Lehen, *22 immigrants died in ICE detention centers during the past 2 years*, NBC NEWS (Jan. 6, 2019), <https://www.nbcnews.com/politics/immigration/22-immigrants-died-ice-detention-centers-during-past-2-years-n954781> [<https://perma.cc/R6XF-AFLZ>].

<sup>204</sup> U.S. CUSTOMS AND BORDER PROT., *At Points of Entry*, U.S. DEPT. OF HOMELAND SECURITY (Apr. 2, 2018), <https://www.cbp.gov/border-security/ports-entry> (“CBP provides security and facilitation operations at 328 points of entry throughout the country.”).

<sup>205</sup> *See, e.g.*, Nick Miroff & Robert Moore, *7-year old migrant girl taken into Border Patrol Custody dies of dehydration, exhaustion*, WASH. POST (Dec. 13, 2018), [https://www.washingtonpost.com/world/national-security/7-year-old-migrant-girl-taken-into-border-patrol-custody-dies-of-dehydration-exhaustion/2018/12/13/8909e356-ff03-11e8-862a-b6a6f3ce8199\\_story.html?noredirect=on&utm\\_term=.7678aa4e3579](https://www.washingtonpost.com/world/national-security/7-year-old-migrant-girl-taken-into-border-patrol-custody-dies-of-dehydration-exhaustion/2018/12/13/8909e356-ff03-11e8-862a-b6a6f3ce8199_story.html?noredirect=on&utm_term=.7678aa4e3579) [<https://perma.cc/M4XW-N2M5>].



conditions in immigration detention that were abysmal.<sup>206</sup> In recent weeks, there have been several deaths that reportedly occurred while individuals were in the custody of CBP.<sup>207</sup>

While a warrant requirement to search electronic devices at the border may result in detention of some aliens, the harm that could result from the detention of aliens while warrants are issued (or not issued) based on probable cause must be balanced against the general harm that could be caused by CBP agents having what amounts to a free pass to forensically search electronic devices at the border with no probable cause or individualized suspicion. While ideally aliens should be able to enjoy an expectation of privacy at the border that is the same as inside the United States without foregoing other personal liberties, the harm that could be caused by CBP agents' searching electronics without probable cause is arguably greater than the harm caused by detention for a few days.<sup>208</sup>

#### ii. Harm to Asylum Applicants

The use (or misuse) of information obtained during a forensic search of an alien's electronic device could have disastrous consequences for removable aliens seeking to remain in the United States to pursue asylum claims. For example, under current U.S. immigration law, asylum applicants bear the burden of proof to establish that they are fleeing persecution in their home country on account of "race, religion, nationality, membership in a particular social group, or political opinion."<sup>209</sup> It is reasonable to imagine a regime in which a migrant's text message to a family member expressing a desire to return to the home country in the future could be used as evidence that the applicant is not really fleeing persecution. There is a wealth of personal and private information that could be easily garnered through a forensic search and weaponized against immigrants seeking entry to the United States, even though their claims for asylum may be legitimate.

Another example of how information seized from an asylum applicant's smartphone could harm the alien's access to immigration relief is in cases of alleged smuggling—a ground for inadmissibility to the United States.<sup>210</sup> Under the INA, "[a]ny alien who at any time knowingly has encouraged, induced, assisted, abetted, or aided any other alien to enter or to try to enter the United States in violation of law is inadmissible."<sup>211</sup> In the realm of smuggling, there are many hypothetical scenarios in which text message conversations could be entered into evidence against an asylum applicant. For example, if the applicant

---

<sup>206</sup> See, e.g., Andrew Gumbel, 'They were laughing at us': immigrants tell of cruelty, illness and filth in US detention, THE GUARDIAN (Sept. 12, 2018), <https://www.theguardian.com/us-news/2018/sep/12/us-immigration-detention-facilities> [<https://perma.cc/6Z38-KPZ6>].

<sup>207</sup> See Seville, Rappleye & Lehren, *supra* note 203.

<sup>208</sup> *Id.*

<sup>209</sup> 8 U.S.C. § 1158(b)(1)(B) (2009).

<sup>210</sup> 8 U.S.C. § 1182(a)(6)(E)(i) (2013).

<sup>211</sup> *Id.*

talks about saving money to bring the child to the U.S., the government could use this as evidence of “encouraging” smuggling.<sup>212</sup> There could also be scenarios in which sending innocuous messages to allegedly gang-affiliated family members or friends could be enough for CIS/EOIR to accuse an individual of being gang-affiliated, which could be grounds for inadmissibility and undermine the applicant’s ability to seek immigration relief in the U.S.<sup>213</sup> The stakes are high for privacy at the border for citizens and non-citizens alike, but the consequences for individuals seeking asylum in the U.S. are arguably even higher.

## VI. CONCLUSION

Forensic searches of electronic devices at the border are fundamentally different from the routine searches imagined by the Framers when they created the border search exception. As electronic devices become more and more omnipresent, allowing the border search exception to extend to forensic searches of electronic devices opens up new avenues for invasions of privacy that are fundamentally at odds with the Fourth Amendment’s reasonableness requirement. Given the depth and breadth of the information that can be uncovered through forensic device searches, the Supreme Court should require a warrant based on probable cause to perform such a search. Though a warrant requirement may still provide imperfect privacy protections to non-citizens at the border, it is preferable to a rule that allows border officials the ability to conduct intrusive forensic searches with impunity and without cause.

---

<sup>212</sup> *Id.*

<sup>213</sup> See The Immigrant Legal Resource Center, *Practice Advisory: Understanding Allegations of Gang Membership/Affiliation in Immigration Cases*, THE IMMIGRANT LEGAL RES. CTR. 1, 9 (Apr. 2017), [https://www.ilrc.org/sites/default/files/resources/ilrc\\_gang\\_advisory-20170509.pdf](https://www.ilrc.org/sites/default/files/resources/ilrc_gang_advisory-20170509.pdf) (“There is no ground of inadmissibility in the Immigration and Nationality Act (INA) that specifically bars persons who are or were gang members from being admissible. Nonetheless, if the individual applying for an immigration benefit is not otherwise inadmissible and DHS alleges the person to be a former or current gang member, DHS may argue that such person triggers the security or terrorism related grounds of inadmissibility found at INA § 212(a)(3)(B).”).