

# Washington and Lee Journal of Civil Rights and Social Justice

Volume 27 | Issue 1 Article 6

Fall 2020

# GPS Tracking at the Border: A Mistaken Expectation or a Chilling Reality

Kimberly Shi Washington and Lee University School of Law, shi.k21@law.wlu.edu

Follow this and additional works at: https://scholarlycommons.law.wlu.edu/crsj

Part of the Civil Rights and Discrimination Commons, Criminal Law Commons, Criminal Procedure Commons, Fourth Amendment Commons, and the Human Rights Law Commons

#### **Recommended Citation**

Kimberly Shi, *GPS Tracking at the Border: A Mistaken Expectation or a Chilling Reality*, 27 Wash. & Lee J. Civ. Rts. & Soc. Just. 161 (2020).

Available at: https://scholarlycommons.law.wlu.edu/crsj/vol27/iss1/6

This Note is brought to you for free and open access by the Washington and Lee Journal of Civil Rights and Social Justice at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Journal of Civil Rights and Social Justice by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact <a href="mailto:christensena@wlu.edu">christensena@wlu.edu</a>.

# **GPS Tracking at the Border: A Mistaken Expectation or A Chilling Reality**

Kimberly Shi<sup>\(\Delta\)\*</sup>

#### Abstract

In 2018, Matthew C. Allen, the Assistant Director for the Domestic Operations Division within the United States Department of Homeland Security, filed a declaration in United States v. Ignjatov describing a departmental policy allowing for the installation of a "GPS tracking device on a vehicle at the United States border without a warrant or individualized suspicion," limited "to 48 hours." While the Border Search Doctrine, which predates the Fourth Amendment, deems that no warrant is necessary at the border for most searches and seizures because of the government's inherent power to control who or what comes within a nation's borders, the Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." This Note examines the implications of the installation of a Global Positioning Services (GPS) tracking device at the border without a warrant and whether the installation and tracking thereafter should be considered a constitutional exception under the Border Search Doctrine, unconstitutional based on Fourth Amendment precedent, or both. This Note highlights the tension between "classic" Fourth Amendment jurisprudence and the Border Search Doctrine as a result of technological advancement, and determines based on current policies and precedent, such as United States v.

Δ 2020 Louise A. Halper Award Winner for Best Student Note

<sup>\*</sup> Candidate for J.D., May 2021, Washington and Lee University School of Law. I would like to extend my sincerest appreciation and gratitude to everyone who helped me throughout the Note writing process. I would like to particularly thank my faculty advisor Alexandra Klein, who spent countless hours assisting me every step of the way. This Note would not have been published without all of the comments and critiques provided by her and numerous other individuals. Finally, I would also like to thank my friends and family for all of their support and patience over the years. Thank you.

Jones and Carpenter v. United States, that the installation of a GPS tracking device is a search under the Fourth Amendment and not subject to the Border Search Doctrine exception. This Note then concludes by advocating for greater policy transparency in congruence with established precedent in order to ensure the privacy rights of both citizens and noncitizens alike moving forward.

# Table of Contents

I. Introduction	163
II. Background	168
A. The Fourth Amendment	
B. Border Search Doctrine	179
1. Routine v. Non-Routine Searches	
2. Extended Border Search	
3. Reasonable Suspicion, Time and Distance	
4. Border Search Policies Known to Date	
III. The Tension Between the Fourth Amendment and the Bo	rder
Search Doctrine	
A. GPS Tracking & Its Place in The Fourth Amendment	
1. United States v. Ignjatov	
B. Unknown Policies & Ongoing Electronic Frontier	
Foundation Suit	
IV. GPS Devices & Current Border Policies	200
A. Classic Fourth Amendment Interpretation	
B. Applying the Border Search Doctrine	
1. GPS device in a Routine v. Non-Routine Context	
V. Transparency and Accountability: Why Courts Matter	219
VI. Conclusion	228

#### I. Introduction

In 2017, border patrol agents attached two GPS tracking devices to a truck and trailer crossing the U.S. border. Acting without a warrant, federal agents tracked the vehicles on their computers for the next thirty-three hours as the truck made its way to Los Angeles.<sup>2</sup> Law enforcement utilized electronic surveillance until the defendants drove from San Bernardino County to Los Angeles County.<sup>3</sup> Then, a combination of physical surveillance and electronic monitoring began. 4 After more than twenty-one hours of surveillance, a Los Angeles Police Department (LAPD) officer witnessed the defendants get out of the vehicle and meet an unknown man.<sup>5</sup> The unknown man retrieved a small duffle bag and handed it to one of the defendants before both parties departed.<sup>6</sup> The officers believed that the defendants were key individuals in a drug trafficking organization and that the duffle bag contained cocaine. Yet when the officers approached the defendants and detained them on suspicion of possession of a controlled substance with an intent to transport, they only found

<sup>1.</sup> See Complaint for Injunctive Relief at 1, Elec. Frontier Found. v. Dep't of Homeland Sec., No. 1:19-cv-02578 (D.C.C. Aug. 27, 2019), ECF No. 1 [hereinafter EFF Complaint] (laying out the facts from United States v. Ignjatov, No. 5:17-cr-00222-JGB (C.D. Cal. Oct. 30, 2017), ECF No. 1 and the failed attempts by the Electronic Frontier Foundation in filing FOIA requests to CBP and ICE for information regarding GPS policies at the border).

<sup>2.</sup> See Complaint at 13–19, United States v. Ignjatov, No. 5:17-cr-00222-JGB (C.D. Cal. Oct. 30, 2017), ECF No. 1 [hereinafter Ignjatov Complaint] (documenting email exchanges between LAPD officials and FBI agents and revolving around tailing the vehicle).

<sup>3.</sup> See id. (discussing how border agents believed the warrantless installation at the border to be valid).

<sup>4.</sup> See id. (describing how Agent Asatur and Agent Monroe assisted in the surveillance both before and at the time of arrest).

<sup>5.</sup> See Declaration of Asatur Mkrtchyan at 3–4, United States v. Ignjatov, No. 5:17-cr-00222-JGB (C.D. Cal. May 21, 2018), ECF No. 87-2 [hereinafter Asatur Declaration] (outlining his knowledge and facts of the case as well as his experience as a police officer for the LAPD).

<sup>6.</sup> See id. at 2 (describing how law enforcement officers seized ten duffle bags of cocaine from another Bo-Mak semi-truck driven by "Karac" after officers saw him receive the bags from a co-conspirator).

<sup>7.</sup> See id. at 3–4 (explaining how the agents utilized the location data to intercept the Bo-Mak truck and proceeded to tail it).

fifteen four-pound packages of sugar in the duffle bag.<sup>8</sup> Federal agents released the defendants following the search but later arrested the defendants as they attempted to leave the United States for Canada in Port Huron, Michigan for conspiracy to traffic cocaine.<sup>9</sup> This was eight days after the initial installation of the tracking device.<sup>10</sup>

Ruling consistently with *United States v. Jones*, <sup>11</sup> the district court found the "[s]urreptitious surveillance of an individual's movement through placement of a GPS device on a vehicle [to] implicate[] far greater privacy concerns than the physical integrity of the vehicle." <sup>12</sup> The combination of the installation with the "subsequent tracking of data over a prolonged period away" from the border could not be justified under the border search exception. <sup>13</sup> The court then suppressed all of the evidence garnered from the physical and electronic surveillance of the defendants. <sup>14</sup>

<sup>8.</sup> See id. (explaining that Ignjatov and the other defendant consented to the search at this time).

<sup>9.</sup> See Ignjatov Complaint, supra note 2, at 19 (outlining the drug trafficking investigation and the reasonable suspicion for the arrest based on Hannah Monroe's declaration); see also Declaration of Hannah Monroe at 7–8, United States v. Ignjatov, No. 5:17-cr-00222-JGB (C.D. Cal. May 21, 2018), ECF No. 87-1 [hereinafter Monroe Declaration] (describing in detail the arrest and surveillance measures used after the installation of the GPS device).

<sup>10.</sup> See Declaration of Steven Gruel at 9, United States v. Ignjatov, No. 5:17-cr-00222-JGB (C.D. Cal. June 18, 2018), ECF No. 95 [hereinafter Gruel Declaration] (noting how the use of GPS tracking devices encompassed from the time of installation on October 20, 2017 till the defendants' arrest on October 28, 2017, meaning that "law enforcement tracked the defendants across the country over thousands of miles continuously for over eight days primarily only using the GPS monitoring device").

<sup>11.~</sup>See United States v. Jones, 565 U.S. 400, 402-03 (2012) (holding that the installation of a GPS tracking device without a warrant violated the Fourth Amendment).

<sup>12.</sup> See Am. Order Granting Defendants' Mot. to Suppress at 7, United States v. Ignjatov, No. 5:17-cr-00222-JGB (C.D. Cal Oct. 10, 2018), ECF No. 132 [hereinafter Amended Order] (granting the defendants' motion to suppress evidence after considering the oral argument and the papers filed both in support of, and in opposition to, the motion).

<sup>13.</sup> See id. at 7–8 (analyzing the instillation under the Border Search and Extended Border Search doctrine).

<sup>14.</sup> See id. at 15 (concluding that the defendants' motion to suppress should be granted).

This case, *United States v. Ignjatov*,<sup>15</sup> revealed an unknown Department of Homeland Security (DHS) and Customs and Border Protection (CBP) policy to the general public.<sup>16</sup> According to a declaration from Assistant Director Matthew C. Allen, Homeland Security's policy (DHS GPS Policy) allows for the installation of a "GPS tracking device on a vehicle at the United States border without a warrant or individualized suspicion."<sup>17</sup> Because the warrantless tracking and monitoring policy is "limit[ed] [to] warrantless GPS monitoring to 48 hours," DHS deemed it acceptable because individuals have "a significantly reduced expectation of privacy in the location of their vehicles" at the border.<sup>18</sup> This forty-eight hour rule also purportedly "did not apply to commercial vehicles like semi-trucks whatsoever," for according to Assistant Director Allen, "a significantly reduced expectation of privacy in the location of [these] vehicles appl[ies]."<sup>19</sup>

To date, DHS and CBP refuse to provide further explanation and insight into this DHS GPS Policy.<sup>20</sup> The Electronic Frontier Foundation (EFF) filed suit against DHS after DHS denied EFF's FOIA request.<sup>21</sup> EFF hopes to shed more light on this policy, but

<sup>15.</sup> United States v. Ignjatov, No. 5:17-cr-00222-JGB (C.D. Cal. Oct. 12, 2018), ECF No. 134 (granting government's motion to dismiss the case as to Slavco Ignjatov).

<sup>16.</sup> See Gruel Declaration, supra note 10, at 2–4, 8–10 (explaining how this 48-hour policy is unheard of but the agents acted based on this knowledge and assumption).

<sup>17.</sup> See Declaration of Assistant Director Matthew C. Allen at 2–3, United States v. Ignjatov, No. 5:17-cr-00222-JGB (C.D. Cal. Sept. 28, 2018), ECF No. 125 [hereinafter Allen Declaration] (providing a formal statement as the "Assistant Director for the Domestic Operations Division within the U.S. Department of Homeland Security (DHS) . . . U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI)").

<sup>18.</sup> See id. (providing no other explanation regarding the authority behind the policy or when it came into fruition).

<sup>19.</sup> See Gruel Declaration, supra note 10, at 2 (noting that according to agents Gernatt and Abair "warrantless GPS installation was permitted as long as monitoring did not exceed 48 hours . . . [and] this '48 rule' did not apply to commercial vehicles like semi-trucks whatsoever"); Allen Declaration, supra note 17, at 1–3.

<sup>20</sup>. See Ignjatov Complaint, supra note 2, at 1-6 (denying and refusing to respond to EFF's FOIA request).

 $<sup>21.\ \</sup> See$  id. (laying out the requests EFF made to CBP and ICE regarding these policies).

the suit is ongoing.<sup>22</sup> The ambiguity of this policy is problematic because it highlights a juncture between Supreme Court precedent and Fourth Amendment jurisprudence that could potentially implicate significant privacy concerns for both citizens and noncitizens alike.<sup>23</sup>

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."<sup>24</sup> This protection is not limited to merely an intrusion on property.<sup>25</sup> Instead, it protects a person's "reasonable expectation of privacy" that society also recognizes as reasonable.<sup>26</sup> Warrants are therefore necessary in almost all instances for a valid search to occur.<sup>27</sup> The Border Search Doctrine, however, is one of the few exceptions to this general rule.<sup>28</sup>

<sup>22.</sup> See Order, Elec. Frontier Found. v. Dep't of Homeland Sec., No. 1:19-cv-02578 (D.C.C. Aug. 6, 2020), ECF No. 15 [hereinafter EFF Order] (setting deadlines for plaintiff and defendant's motions for summary judgment).

<sup>23.</sup> See id. (challenging the withholding of information that could potentially result in "circumvention of the law").

<sup>24.</sup> U.S. CONST. amend. IV.

<sup>25.</sup> See Katz v. United States, 389 U.S. 347, 357 (1967) (deciding that the Fourth Amendment protects people rather than places); see also United States v. Jones, 565 U.S. 400, 414 (2012) (identifying that a physical intrusion for the purpose of seeking information is considered a search under the Fourth Amendment).

<sup>26.</sup> See Katz, 389 U.S. at 361–62 (Harlan, J., concurring) (creating a two part test requiring a subjective component, where the court evaluates whether the individual had a reasonable expectation of privacy, and an objective component, where the court evaluates whether the expectation is one that society recognizes as reasonable); see also Smith v. Maryland, 442 U.S. 735, 735 (1979) (determining that the installation of a pen register by law enforcement to not be a search within the meaning of the Fourth Amendment because consumers could be aware of an assumption of risk).

<sup>27.</sup> See Riley v. California, 573 U.S. 373, 381–83 (2014) (holding that police must obtain a warrant before searching a cell phone incident to arrest and a warrantless search to be unconstitutional); see also Katz, 389 U.S. at 357 (mentioning how warrantless searches are typically unlawful "subject only to a few specifically established and well-delineated exceptions").

<sup>28.</sup> See YULE KIM, CONG. RESEARCH SERV., RL31826, PROTECTING THE U.S. PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT, 6–19 (2009) [hereinafter KIM, PROTECTING THE U.S. PERIMETER] (addressing the scope of government's constitutional authority at the border); see United States v. Ramsey, 431 U.S. 606, 619 (1977) (discussing how the Fourth Amendment's power came from deterrence and security efforts).

The Border Search Doctrine predates the Fourth Amendment and derives its powers from Congress's inherent authority to regulate commerce and enforce immigration laws.<sup>29</sup> No warrant is necessary at the border for most searches and seizures because of the government's inherent power to control who or what comes within a nation's borders.<sup>30</sup> This is an intrinsic attribute of national sovereignty.<sup>31</sup> The Fourth Amendment's balance of interests thus leans heavily in favor of the government at the border.<sup>32</sup> Even though courts favor government interests at the border, searches and seizures must remain "reasonable" dependent on the facts and circumstances in question.<sup>33</sup>

While the Border Search Doctrine falls under one of the warrantless exceptions of the Fourth Amendment, the scope of authority remains hazy in application and is up to the interpretation of law enforcement and courts around the country, posing problematic inconsistencies.<sup>34</sup> This Note specifically focuses

<sup>29.</sup> See 19 U.S.C. § 482 (2002) (establishing "officers or persons authorized to board or search vessels may stop, search, and examine . . . any vehicle, beast, or person"); see also 19 U.S.C. § 1582 (1930) (discussing the Tariff Act of 1930 and outlining the ability of the Secretary of Treasury to prescribe regulations to the search of persons and baggage); see also Ramsey, 431 U.S. at 619 (detailing how the border search exception has a history as old as the Fourth Amendment, and the broad powers originally granted was to regulate "Commerce with foreign Nations" and to "prevent smuggling" and "prohibited articles from entry").

 $<sup>30.\ \</sup> See\ Ramsey,\ 431\ U.S.$  at 619 (elaborating on the broad powers granted by Congress).

<sup>31.</sup> See id. at 616 (providing explicit examples from the state legislatures on Sept. 25, 1789 and the Act of July 31, 1789 to show that there is an "acknowledgement of plenary customs power" which is "differentiated from the more limited power to enter and search" a particular place, where a warrant is required).

<sup>32.</sup> See United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (dictating that "[s]ince 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").

<sup>33.</sup> See Almeida-Sanchez v. United States, 413 U.S. 266, 267–76 (1973) (determining that the search of the petitioner's automobile by a roving patrol at least twenty miles north of the Mexican border was unreasonable due to an absence of probable cause or consent).

<sup>34.</sup> See Allen Declaration, supra note 17, at 2–3 (revealing through a declaration from a Homeland Security official that it was a known policy for DHS to be allowed to install a warrantless tracking device as long as it was for less than 48 hours upon entry into the United States); see also J. Alan Bock, Annotation, Validity of border searches & seizures by customs officers, 6 A.L.R. Fed. 317 (1971) (providing an analysis of the different positions circuits have

on whether the use of a Global Positioning Services (GPS) tracking device at the border without a warrant should fall under the Border Search Doctrine, or if it should fall in line with *United States v. Jones*,<sup>35</sup> in which the Supreme Court held unanimously that it was unconstitutional under the Fourth Amendment to use a GPS tracking device without a warrant to monitor and gather information on an individual.<sup>36</sup>

Part II provides background on the Fourth Amendment and the Border Search Doctrine, while discussing the rationales for its expansion over the years.<sup>37</sup> It highlights the difficulties in differentiating between warrantless searches of automobiles to other items, such as electronic devices. 38 Part III discusses United States v. Ignjatov to highlight the tension between "classic" Fourth Amendment jurisprudence and the Border Search Doctrine, while discussing the ramifications of the policy guidelines revealed.<sup>39</sup> Part IV analyzes whether the installation of a GPS tracking device should fall under "classic" Fourth Amendment protections, the Border Search Doctrine, or both.<sup>40</sup> Part V offers reasons for why such an inconsistency between policy and precedent is detrimental to privacy concerns and advocates the position that policy transparency in congruence with established precedent is necessary to ensure that the privacy rights of both citizens and noncitizens in the United States remain intact. 41

#### II. Background

Fourth Amendment jurisprudence has evolved with advancements in technology.<sup>42</sup> This evolution results in

taken in regard to searches and seizures).

- 35. United States v. Jones, 565 U.S. 400, 401 (2012).
- 36. See id. at 401, 408–11 (concluding that the common-law trespass doctrine applied to the case rather than Katz's reasonable expectations test).
  - 37. See discussion infra Sections II.A.-B.
  - 38. See discussion infra Part II.
  - 39. See discussion infra Sections III.A-B.
  - 40. See discussion infra Sections IV.A–B.
  - 41. See discussion infra Part V.
- 42. See Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 MICH. L. REV. 801, 805 (2004) (discussing how courts "must update and redefine the Fourth Amendment as

complications in applying existing Fourth Amendment doctrines here and a greater chance of the deterioration of individual privacy. <sup>43</sup> This section summarizes the development and use of the reasonable expectation test in the Fourth Amendment context. It highlights its application in regard to tracking on public roadways to the ultimate tracking of the vehicle itself. This section also highlights special considerations courts analyze in circumstances where the level of intrusiveness heightens privacy concerns.

#### A. The Fourth Amendment

The Fourth Amendment protects individuals from unreasonable government searches and seizures. 44 Seizures can be split into two categories. 45 A seizure of property is "some meaningful interference with an individual's possessory interests in that property." 46 In contrast, seizure of an individual occurs when an individual reasonably believes that he or she is not at liberty to leave a government official's presence, given all of the circumstances surrounding the incident. 47 Courts balance these elements to determine whether the government action was reasonable. 48

technology evolves).

- 43. See Tracey Maclin, The Central Meaning of the Fourth Amendment, 35 WM. & MARY L. REV. 197, 197–202 (1993) (deliberating the conception of "a man's home is his castle" in the Fourth Amendment context).
- 44. See U.S. CONST. amend. IV (declaring the right of the people to "be secure in their persons, houses, papers, and effects . . . .").
- 45. See infra notes 46–47 and accompanying text (describing different circumstances where Courts evaluate what constitutes a "search" under the Fourth Amendment).
- 46. See United States v. Jacobsen, 466 U.S. 109, 113 (1984) (holding that the removal of a tube from a box, after federal agents observed a white powdery substance, did not constitute as a search under the Fourth Amendment because no reasonable expectation was expected).
- 47. See Sodal v. Cook County, 506 U.S. 56, 61 (1992) (finding the dispossession of mobile homeowners of their mobile home by deputy sheriffs to be a "seizure" within the Fourth Amendment because the home was literally carried away).
- 48. See Kim, Protecting the U.S. Perimeter, supra note 28 (explaining that reasonableness is determined by "balancing the governmental interest justifying the intrusion against a person's legitimate expectation of privacy").

In contrast, warrantless searches under the Fourth Amendment are typically per se unreasonable. 49 The Supreme Court decided in *Katz v. United States*<sup>50</sup> that the attachment of an eavesdropping device outside of a public phone booth constituted an unreasonable search.<sup>51</sup> By listening and recording the petitioner's words, the government "violated the privacy on which [the petitioner] justifiably relied" and thus constituted a search and seizure under the Fourth Amendment.<sup>52</sup> Justice Harlan's concurrence developed a two-prong test to determine whether a search occurred.<sup>53</sup> If an individual has a subjective expectation of privacy over the domain in question and society objectively recognizes that expectation as reasonable, then the search is unconstitutional unless law enforcement acquired a warrant or one of the exceptions to the warrant requirement applies.<sup>54</sup> This is because "[t]he Fourth Amendment [] protects people and not places."55 Courts now apply this "reasonable expectation" of privacy test in Fourth Amendment cases.<sup>56</sup>

As technology advanced, Courts faced a new challenge in determining searches in the public and private domain. In *United* 

<sup>49.</sup> See id. (describing how violations of the Fourth Amendment occur when the government fails to justify the intrusion of a person's privacy expectations).

<sup>50.</sup> Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the Government's use of an electronic listening device constituted a search under the Fourth Amendment).

<sup>51.</sup> See id. at 355–57 (explaining that Fourth Amendment protections should not be based on the "presence or absence of a physical intrusion into any given enclosure" and that a new test would replace the test for privacy due to technological advancement).

<sup>52.</sup> See id. at 353 (finding that the "fact that the electronic device . . . did not penetrate the wall of the booth" to have no "constitutional significance").

<sup>53.</sup> See id. at 360–62 (Harlan, J., concurring) (agreeing with the majority opinion "that an enclosed telephone booth is an area" like a home but there should be a subjective and objective test as to whether there is an expectation of privacy).

<sup>54.</sup> *See id.* (developing the "reasonable expectation of privacy" test requiring both a subjective and objective component).

<sup>55.</sup> See id. at 351 (majority opinion) (describing how even if an individual discloses information in public, if it is a disclosure he reasonably hopes to keep private, then it remains constitutionally protected).

<sup>56.</sup> See United States v. Knotts, 460 U.S. 276, 286 (1983) (finding no violation with the installation); see also United States v. Karo, 468 U.S. 705, 706 (1984) (concluding no violation under the *Katz* test occurred for there was no violation to an individual's reasonable expectation of privacy).

States v. Knotts,<sup>57</sup> the Supreme Court concluded that the surveillance, tracking, and following of an individual traveling on a public roadway did not constitute as a search or seizure.<sup>58</sup> The "beeper" placed inside the chloroform container was a radio transmitter, which transmitted beeper signals to a monitor held by law enforcement.<sup>59</sup> Law enforcement obtained consent from the original owner prior to the installation of the beeper for tracking purposes; however, officials failed to obtain a warrant prior to using the beeper to monitor Knotts. 60 The Court, however, concluded that no reasonable expectation of privacy exists on public roadways because of the ability of any individual to survey those movements freely.<sup>61</sup> While it did not apply to the case before the Court, Justice Brennan's concurrence clarified the Supreme Court's statement in *Katz* regarding "[t]he Fourth Amendment [] protect[ing] people and not places," by explaining that "when the Government does engage in [the] physical intrusion of a constitutionally protected area to obtain information, that intrusion may constitute a violation of the Fourth Amendment."62 The Court also left open the question of the duration of government

<sup>57.</sup> See Knotts, 460 U.S. at 276 (becoming one of the most important electronic monitoring cases in Fourth Amendment precedent).

<sup>58.</sup> See id. at 276–77 (holding that even though the officers did not only rely on visual surveillance, the use of a beeper did not change the fact that the Fourth Amendment does not prohibit law enforcement from "augmenting their sensory faculties" and the beeper did not change what "would not have been visible to the naked eye from outside the cabin").

<sup>59.</sup> See id. at 276 (determining no violation of privacy even with the beeper because the vehicle traveled on public roadways).

<sup>60.</sup> See id. at 277–81 (noting that the record did "not reveal that the beeper was used after the location in the area of the cabin had been initially determined" by a combination of physical and electronic surveillance).

<sup>61.</sup> See id. at 276 (reasoning that there is no reasonable expectation of privacy for individual's traveling on public roads because of the ability to observe their movements freely, even though a radio transmitter was placed into a drum purchased by one of the codefendants).

<sup>62.</sup> See id. at 286 (Brennan, J., concurring) (describing how Katz did not erode the principle of the Fourth Amendment affording protections to property and explaining how the case would have been a much more difficult one to decide if the respondent had challenged the original installation of the beeper rather than "merely certain aspects of the monitoring of the beeper installed in the chloroform container purchased by respondent's compatriot").

surveillance required for Fourth Amendment protections to apply, leaving it to be dealt with in the future.<sup>63</sup>

Similarly, the Supreme Court in *United States v. Karo*<sup>64</sup> held that the warrantless use of an electronic monitor within a container was reasonable and did not infringe on Karo's interests within the meaning of the Fourth Amendment.<sup>65</sup> The Court concluded that the use of the beeper did not trigger Fourth Amendment protections because the beeper merely led law enforcement agents to the storage facility without identifying the specific locker, which was identified only by the smell of ether emanating therefrom.<sup>66</sup> Similar to *Knotts*, the Court maintained that no reasonable expectation of privacy exists on public roadways.<sup>67</sup> Therefore, as long as an individual is visible and traversing on public streets, then a lower expectation of privacy exists.<sup>68</sup>

<sup>63.</sup> See id. at 283–84 (majority opinion) (discussing how the Respondent "expresses the generalized view that the result of the holding sought by the government would be that 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision," but "if such dragnet type of law enforcement practices as a respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable").

<sup>64.</sup> United States v. Karo, 468 U.S. 705, 706 (1984).

<sup>65.</sup> See id. at 706–07 (finding that the "informant's consent was sufficient to validate the installation," and any transfer thereafter was not a search or seizure since no conveyance of information of private information occurred and possessory interests were not interfered with in any meaningful way).

<sup>66.</sup> See id. (determining that the use of the beeper to locate the storage facility did not amount to an illegal search but acknowledging that there is a reasonable expectation of privacy from being monitored within the privacy of one's home).

<sup>67.</sup> See id. (deciding that the use of the beeper to locate the storage facility did not equate to an illegal search because "the ether was seen being loaded into [the] truck, which then traveled the highways").

<sup>68.</sup> See id. at 712–13 (discussing how the only privacy interests infringed were due to the occasional monitoring of the beeper which did not constitute a violation of Fourth Amendment protections and similarly, even though the can "may have contained an unknown and unwanted foreign object," there was no intrusion on possessory interest in a meaningful way and at most, it "was a technical trespass on the space occupied by the beeper"). The Supreme Court established an automobile exception to the warrant requirement in Caroll v. United States, 267 U.S. 132, 134–36, 153 (1925), but because this Note focuses on tracking rather than the flexibility of law enforcement in the vehicle context, no further discussion on this exception follows.

The Supreme Court in *United States v. Jones* held that law enforcement committed a search by attaching a GPS tracking device to a vehicle. <sup>69</sup> The Court came to this result even though the device was utilized to monitor the individual on public streets. <sup>70</sup> The Court decided that it "need not address the Government's contention that Jones had no 'reasonable expectation of privacy,' because Jones's Fourth Amendment rights [did] not rise or fall with the *Katz* formulation."

The Court focused instead on the idea of intrusion. The Jones Court differentiated Jones from Karo and Knotts because in Jones, the Government "trespassorily inserted the information-gathering device" onto the private property of an individual. Since the Government "physically occupied private property for the purpose of obtaining information," the encroachment and intrusion on a protected area constituted a search under the Fourth Amendment. The Court, moreover, expressly distinguished Karo from Jones because in Karo, law enforcement acquired the consent of the original owner prior to the beeper being placed in the container to track the vehicle. The beeper device consequently did not constitute a trespass or intrusion. Jones treated the installation of the GPS and its use to track a vehicle as a singular

<sup>69.</sup> See United States v. Jones, 565 U.S. 400, 401–03 (2012) (affirming the lower court's decision after hearing about how law enforcement attached a GPS tracking device to the car of the defendant's wife in Maryland on the eleventh day and tracked it for 28 days, after obtaining a warrant authorizing the "installation of the device in the District of Columbia [] within 10 days").

<sup>70.</sup> See id. at 401, 409 (explaining how "the Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test" and that since Jones "possessed the Jeep at the time the Government trespassorily inserted the information-gathering device" it is differentiated from Knotts and Karo).

<sup>71.</sup> See id. (determining that because the government intruded on privacy interests, which is a search under the Fourth Amendment, that there was no need to also apply *Katz*).

<sup>72.</sup> See id. at 406–12 (utilizing common-law trespass rather than Katz's expectations test).

<sup>73.</sup> See id. at 408–11 (discussing how Katz did not replace the common-law of trespass).

<sup>74.</sup> *Id.* at 404–05, 411–12.

<sup>75.</sup> See id. at 409 (discussing how the transfer of the container with the beeper "did not convey any information and thus did not invade Karo's privacy").

<sup>76.</sup> See id. (determining that because Karo accepted the beeper, he was "not entitled to object to the beeper's presence").

act that constitutes a search.<sup>77</sup> This reasoning echoed Justice Brennan's concurrence regarding *Katz* in *United States v. Knotts*.<sup>78</sup>

Jones "the held that reasonable-expectation-of-privacy test [] added to, not substituted for, the common-law trespassory test."79 The majority found a strict application of *Katz* to pose greater issues and problematic inconsistencies. 80 In contrast, the concurrences hoped for a stricter application. 81 Justice Alito's concurrence slightly diverged from the majority by focusing more on interest balancing. 82 Utilizing *Knotts*, Justice Alito asserted that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."83 However, GPS "the longer term monitoring investigations...impinges on expectation of privacy."84 Justice Alito concluded that the Court "need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."85 Based on this analysis, an individual's expectation of privacy is impinged somewhere between the initial installation and before four weeks of electronic monitoring.86 Justice Alito posited that the "police

<sup>77.</sup> See id. at 404–05, 411–12 (describing the events that provided a justification for identifying a search).

<sup>78.</sup> See Knotts, 460 U.S. at 286 (Brennan, J., concurring) (describing how Katz still allowed for the Fourth Amendment to afford protections to property and no erosion occurred merely from the idea that the Fourth Amendment protects people rather than property).

<sup>79.</sup> Jones, 565 U.S. at 409, 411.

<sup>80.</sup> See id. (describing how adopting the concurrence's stance would "introduce[] yet another novelty into our jurisprudence").

<sup>81.</sup> See id. at 413–18 (Sotomayor, J., concurring) (acknowledging the problems of technological advancement); see also id. at 418–31 (Alito, J., concurring) (positing that a duration shorter than four weeks of surveillance would likely be a search but four weeks certainly was one).

<sup>82.</sup> See id. at 418–31 (Alito, J., concurring) (discussing how short-term monitoring may be valid under the Fourth Amendment but long-term surveillance goes against an individual's reasonable expectation of privacy).

<sup>83.</sup> *Id.* at 430.

<sup>84.</sup> *Id*.

<sup>85.</sup> Id.

<sup>86.</sup> See id. (concluding that relatively brief monitoring is acceptable while prolonged ones, like this four week surveillance, constituted a search under the Fourth Amendment).

may always seek a warrant" if uncertain "whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment Search."87

Justice Sotomayor's concurrence agrees with Justice Alito in terms with the fact that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."88 This is because GPS monitoring "evades the ordinary checks that constrain abusive law enforcement practices."89 However, unlike Justice Alito's position, Justice Sotomayor's concurrence drew a firmer line. 90 Justice Sotomayor premised that "[a]wareness that the Government may be watching chills associational and expressive freedoms," and "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."91 Given the quantity of personal information disclosed to third parties in the digital age, Justice Sotomayor's concurrence did not believe that "all information voluntarily disclosed to some member of the public for a limited purpose if, for that reason alone, disentitled to Fourth Amendment protection."92 Even though the concurrence hoped for a stricter application by proposing an alternative solution to *Katz* and the majority, the majority chose to leave those "vexing problems" for some future case rather than resolving them in one go.<sup>93</sup>

The Supreme Court reaffirmed *Jones'* concept of intrusion in *Carpenter v. United States*, 94 holding that the warrantless acquisition of cell-site information violated Carpenter's Fourth

<sup>87.</sup> Id. at 430-31.

<sup>88.</sup> Id. at 415 (Sotomayor, J., concurring); id. at 429–30 (Alito, J., concurring).

<sup>89.</sup> *Id.* at 416 (Sotomayor, J., concurring).

<sup>90.</sup> See id. at 413–18 (writing that it may be necessary to reconsider expectation of privacy for information disclosed to third parties).

<sup>91.</sup> *Id*.

<sup>92.</sup> Id. at 418.

<sup>93.</sup> See id. at 412–13 (majority opinion) (refusing to adopt Katz exclusively and adopt the concurrence's view); see also Danielle Keats Citron & David Gray, Addressing The Harm of Total Surveillance: A Reply to Professor Neil Richards, 126 Harv. L. Rev. F. 262, 269–71 (2013) (discussing the privacy implications of mass surveillance without oversight).

<sup>94.</sup> Carpenter v. United States, 138 S. Ct. 2206, 2206–08 (2018).

Amendment right against searches and seizures.<sup>95</sup> The Court refused to extend the "Third Party Doctrine,"<sup>96</sup> where no reasonable expectation of privacy exists for information disclosed to third parties, when individuals did have a reasonable expectation of privacy.<sup>97</sup> Instead, the Court drew from both Justice Alito's and Justice Sotomayor's concurrences in *Jones*.<sup>98</sup> Recognizing "that individuals have a reasonable expectation of privacy in the whole of their physical movements," the Court found that cell-site information implicated greater privacy concerns than did GPS tracking.<sup>99</sup> The Court differentiated cell-site data from bank records and pen register data in its ability to "retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers."<sup>100</sup> This data embodied qualities more similar to GPS monitoring because it showcased an "exhaustive chronicle of location information, unlike the limited

<sup>95.</sup> See id. at 2209–10 (finding the expectation of privacy in the current digital era does not fit perfectly or neatly in existing precedents, resulting in difficulties in application).

<sup>96.</sup> The Third Party Doctrine is the idea that no reasonable expectation of privacy exists for information disclosed to third parties; however, courts will typically look at the degree of intrusiveness and whether it resembles the mosaic theory in order to determine if a search occurred. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010). The mosaic theory is the idea that a search occurs if the method of collection allows law enforcement to acquire an intimate look into an individual's life through his or her day-to-day activities. *Id.* Searches in this particular instance are "analyzed as a collective sequence of steps rather than as individual steps," since each step infringes further into the privacy rights of an individual. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV 311, 320–26 (2012).

<sup>97.</sup> See Carpenter, 138 S. Ct. at 2209-10, 2217-21 (recognizing that "individuals have a reasonable expectation of privacy in the whole of their movements").

<sup>98.</sup> See id. at 2217 (mentioning the Court already recognized that individuals have a reasonable expectation of privacy for the whole of their movements and it is not society's expectation for law enforcement agents to "secretly monitor and catalogue every single movement of an individual's car for a long period").

<sup>99.</sup> See id. at 2210, 2217 (contrasting the implications of cell-site information to the information at issue in *Smith* and *Miller*, noting especially how the progression of technology has evolved the reasonable expectation of privacy traditionally known and CSLI being more intrusive than GPS tracking).

<sup>100.</sup> See id. at 2217–19 (discussing why Smith and Miller should not be extended in this instance to the facts of the Carpenter case); but see id. at 2223–24 (Kennedy, J., dissenting) (disagreeing with the distinction drawn by the majority given the degree of information obtainable through this process).

nature of personal information in *Smith v. Maryland*<sup>101</sup> and *United States v. Miller*. <sup>102</sup> A cell-site information system would allow the Government to gather "near perfect surveillance." <sup>103</sup> As such, it violates an individual's reasonable expectation of privacy as to their whole physical movements. <sup>104</sup> Since the *Carpenter* Court determined seven days of historical cell-site location information (CSLI) obtained from the defendant's wireless carrier constituted a search, <sup>105</sup> the holding narrows the point at which electronic monitoring becomes a search, as discussed in Justice Alito's concurrence in *Jones*. <sup>106</sup> The Court, however, explicitly limited its Fourth Amendment protections to the CSLI and did not extend it to topics not before the Court at that time. <sup>107</sup> Therefore, the *Carpenter* decision illustrates a rather narrow application. <sup>108</sup>

Fourth Amendment protections can thus be differentiated and delineated based on a number of things, such as a reasonable expectation within one's home, the lack of a reasonable expectation of privacy on public roadways, and its application to the acquisition

<sup>101.</sup> See Smith v. Maryland, 442 U.S. 735, 741–46 (1979) (concluding that the installation of a pen register by a telephone company without a warrant to not be a search under the Fourth Amendment since average consumers understood the assumption of risk involved when conveying information to a phone company, regardless of the fact that Smith made calls within his home, no expectation of privacy existed over the numbers he dialed).

<sup>102.</sup> United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that Miller did not have a constitutionally protected interest in the financial records he provided to his bank because information revealed to a third party and then conveyed to the government did not constitute a Fourth Amendment violation); see Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018) (discussing the particular qualities of CSLI that breaches typical normal reasonable expectations of privacy).

<sup>103.</sup> Carpenter, 138 S. Ct. at 2217-19.

<sup>104.</sup> See id. (differentiating between Smith and Miller and the CSLI data collected, while noting how the Government failed to account for technological advancement in their argument).

<sup>105.</sup> See id. at 2214–19 (finding that the "retrospective quality of the data here gives police access to a category of information otherwise unknowable").

<sup>106.</sup> See United States v. Jones, 565 U.S. 400, 430–31 (2012) (Alito, J., concurring) (discussing that there was no need to identify "the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark").

<sup>107.</sup> See Carpenter, 138 S. Ct. at 2206, 2217–19 (noting that the application of *Smith* and *Miller* remain undisturbed by the holding in *Carpenter*).

<sup>108.</sup> See id. at 2220–21 (writing that the holding does not extend to matters not before the Court, leaving other types of surveillance for a future time).

and retention of informational data.<sup>109</sup> Warrantless searches are per se unreasonable unless an exception applies.<sup>110</sup> Nonetheless, based on Fourth Amendment precedent alone, the Supreme Court appears to carve a niche for GPS tracking devices and cell-site information, based on the technology's intrusive nature.<sup>111</sup> While the majority in *Jones* focused only on the nature of the intrusion and refused to draw a hardline rule regarding extensive monitoring,<sup>112</sup> Carpenter harped on the degree of intrusiveness and an individual's expectation of privacy in the whole of their physical movements.<sup>113</sup> Based on these rulings, it appears that a device's level of intrusiveness and impediment on privacy remain special considerations in Fourth Amendment precedent.<sup>114</sup>

As Fourth Amendment precedent evolves with technological innovations and attempts to grapple with the fact that "physical intrusion is now unnecessary to many forms of surveillance," <sup>115</sup> the Supreme Court determines and establishes certain exceptions to the Fourth Amendment to balance the interest of the government

<sup>109.</sup> See cases cited supra notes 11, 25, 56, 64, 69, 94 (highlighting the different ways in which Fourth Amendment protections can be wielded).

<sup>110.</sup> See United States v. Ramsey, 431 U.S. 606, 616 (1977) (describing that "as a general principle searches and seizures made at the border are reasonable simply by virtue of the fact that they occur at the border").

<sup>111.</sup> See Jones, 565 U.S. at 404–05, 411–12 (determining the installation of a GPS device to be a trespass and thus a search); see also Carpenter v. United States, 138 S. Ct. 2206, 2210, 2217–19 (2018) (determining that obtaining seven days of CSLI is a search).

<sup>112.</sup> See United States v. Jones, 565 U.S. 400, 404–05, 411–12 (2012) (unwilling to determine broader surveillance issues and focused solely on the trespass).

<sup>113.</sup> See Carpenter, 138 S. Ct. at 2210, 2217–19 (reiterating the concurrences in *Jones* regarding an expectation of privacy even with advancements in technology).

<sup>114.</sup> See id. (finding CSLI to concern greater privacy concerns than GPS tracking); see also Jones, 565 U.S. at 404–05, 411–12 (highlighting that common-law trespass still applies).

<sup>115.</sup> Jones, 565 U.S. at 424–27 (Alito. J., concurring).

with the protection of an individual's privacy. <sup>116</sup> The Border Search Doctrine is one of them. <sup>117</sup>

#### B. Border Search Doctrine

An analysis of the Border Search Doctrine hinges on a number of factors. Due to its convoluted nature, this section breaks down the doctrine based on the location of the search, the type of search, the type of suspicion required, and the border policies known to date.

The Border Search Doctrine is one of the longstanding warrantless search exceptions. Most searches at the border do not require a warrant or probable cause because of Congress's authority to regulate commerce and maintain sovereignty. The border does not merely mean specific checkpoints of entry. It also

<sup>116.</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, 88 (2018) (discussing how the Supreme Court balanced this interest through Terry v. Ohio and United States v. Villamonte-Marquez, where the Court held that a search is constitutional if government interest in the prevention of crime outweighs the intrusion on an individual's Fourth Amendment interests); see also Alison M. Lucier, You Can Judge a Container by Its Cover: The Single-Purpose Exception and the Fourth Amendment, 76 U. Chi. L. Rev. 1809, 1809 (2009) (discussing the single-purpose container exception for warrantless searches); see also Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 HARV. L. Rev. 476, 476–77 (2011) (postulating that the Supreme Court adjusts Fourth Amendment protections in response to changing technology or social practices that expand government power); see Almeida-Sanchez v. United States, 413 U.S. 266, 274 (1973) (describing the balance of interests at the border to favor governmental interests in time of need).

<sup>117.</sup> See United States v. Ramsey, 431 U.S. 606, 616–17 (1977) (illustrating the longstanding right afforded to border agents and searches of this nature at the border).

<sup>118.</sup> See id. (discussing searches at the border to be a "long-standing right of the sovereign to protect itself" and searches of this kind "were not subject to the warrant provisions of the Fourth Amendment and were 'reasonable' within the meaning of the Amendment").

<sup>119.</sup> See id. at 619 (concluding that the ability for border searches to occur stems from the "Constitution giv[ing] Congress broad, comprehensive powers 'to regulate Commerce with foreign Nations," resulting in "reasonable" searches at the border); see also U.S. CONST., ART. I, § 8, cl. 3 (delineating Congress' power of regulation of Commerce between foreign Nations, States and Indian Tribes); see also United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (discussing how interests lean heavily in favor of the government at the border).

<sup>120.</sup> See Almeida-Sanchez, 413 U.S. at 272-73 (providing different examples

includes the "functional equivalent" of a border, which can be described as a point of crossing or port-of-entry. <sup>121</sup> "Actual borders have an international legal status." <sup>122</sup> This, in theory, means that travelers are put on "notice that searches are likely to be made." <sup>123</sup> "Notice diminishes the travelers' expectation of privacy and may make it reasonable to presume that they implicitly [] consented to a warrantless search upon their reentry into the country." <sup>124</sup> Aside from an individual's presence at the border, courts analyze the type and location of the search to determine if a search is constitutional.

#### 1. Routine v. Non-Routine Searches

One factor courts utilize to distinguish border searches is whether the search is "routine" or "non-routine". Routine searches differ from non-routine searches because the latter results in a greater degree of intrusion than the former. A typical

of entry points that could be considered when evaluating a border crossing).

<sup>121.</sup> See id. (indicating that the "permissible scope of intrusiveness of a routine border search might . . . in certain circumstances take place not only at the border itself, but at its functional equivalents," like roads extending from the border).

<sup>122.</sup> See PS Rosenzweig, Functional Equivalents of the Border, Sovereignty, and the Fourth Amendment, 52 U. Chi. L. Rev. 1119, 1133 (1985) [hereinafter PS Rosenzweig, Functional Equivalent] (criticizing the current approaches to the functional equivalence of a border).

<sup>123.</sup> See id. (discussing searches at functional equivalents of a border); see also Schneckloth v. Bustamonte, 412 U.S. 218, 222–27 (1973) (describing the idea that consent is an exception to the warrant requirement); see also Mark R. Santana, Almeida-Sanchez and Its Progeny: The Developing Border Zone Search Law, 17 ARIZ. L. REV. 214, 238 n.149 (1975) [hereinafter Santana, Almeida-Sanchez] (putting forth the idea that one justification for the border zone search is that "when a person leaves the country he is deemed to have implicitly consented to a border search upon his return. Thus, he can reasonably expect to be searched at the point where he enters the nation, whether at an airport, landing pier, or border checkpoint").

<sup>124.</sup> Santana, Almeida-Sanchez, supra note 123, at 238 n.149.

<sup>125.</sup> See United States v. Ramsey, 431 U.S. 606, 618–19 (1977) (discussing how routine searches of entrants do not require reasonable suspicion, probable cause, or a warrant).

<sup>126.</sup> See United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993) (discussing how routine border searches result in a lower degree of privacy invasion and offense to a traveler than nonroutine searches, with one requiring reasonable suspicion to justify it, while the other does not).

routine search could be anything from a pat-down to the removal of outer garments or an x-ray. On the other hand, a non-routine search could include anything from a strip search to other searches going beyond limited intrusions, such as a body cavity search. The key difference is that a non-routine search requires reasonable suspicion while a routine one does not. 129

The Supreme Court explicitly stated in *United States v. Flores-Montano*<sup>130</sup> that the differentiation between "routine" and "non routine" does not apply in the context of vehicular searches. <sup>132</sup> The Supreme Court held that the balancing test, utilized by the lower court, did not apply because "the reasons that might support a suspicion requirement in the case of highly intrusive searches of persons simply do not carry over to vehicles." <sup>133</sup> Instead, because "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border," <sup>134</sup> the Court rejected the assertion that a privacy interest is violated by a suspicionless disassembly of a fuel tank at the border. <sup>135</sup> While

<sup>127.</sup> See United States v. Sandler, 644 F.2d 1163, 1169 (5th Cir. 1981) (affirming and concluding that an "examination of a person by ordinary pat-down or frisk . . . [is] part of the routine examination of a person's effects which require[s] no justification other than the person's decision to cross our national boundary"); see also KIM, PROTECTING THE U.S. PERIMETER, supra note 28 (distinguishing routine and non-routine searches by the differences in the degree of invasion of privacy as well as the degree of the search of the individual).

<sup>128.</sup> See Kim, Protecting the U.S. Perimeter, supra note 28 (breaking down a non-routine search to "include prolonged detentions, strip searches, body cavity searches, and some X-ray examinations," requiring a "reasonable suspicion" prior to conducting the non-routine search).

<sup>129.</sup> See Johnson, 991 F.2d at 1291 (discussing how routine border searches result in a lower degree of privacy invasion and offense to a traveler than non-routine searches, with one requiring reasonable suspicion to justify it, while the other does not).

<sup>130.</sup> United States v. Flores-Montano, 541 U.S. 149, 149 (2004).

<sup>131.</sup> See id. (differentiating between the language used in *United States v. Montoya de Hernandez* for searches on individuals and the searches discussed in the case).

<sup>132.</sup> See id. (determining a different standard for vehicles at the border because of the authority at the border granted by Congress).

<sup>133.</sup> *Id*.

<sup>134.</sup> Ramsey, 431 U.S. at 616.

<sup>135.</sup> See Flores-Montano, 541 U.S. at 149 (discussing how Congress has consistently granted "[e]xecutive 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 into

the Fourth Amendment "protects property as well as privacy," the Government's authority allows for officials to "conduct suspicionless inspections at the border" to protect national sovereignty. This protection and authority includes the ability to "remove, disassemble, and reassemble a vehicle's fuel tank." The Court, however, mentioned that there are instances where "some searches of property are so destructive" or "particularly offensive," to require particularized suspicion. 139

While courts differentiate between a routine and a non-routine search at the border, other considerations exist as the search moves away from the border.

## 2. Extended Border Search

The Border Search Doctrine can also include areas away from the border. An example of this is when the search occurs after entry into the country. Courts deem this an Extended Border Search. An Extended Border Search is more intrusive on the

this country").

136. See id. (recognizing that courts lean heavily in favor of governmental interests at the border).

137. Id. at 149-50.

138. *Id.* As for what constitutes as an "offensive" manner, it remains an open question for courts to determine. See for example, Amended Order, *supra* note 12, at 5. The Ninth Circuit established two factors to determine if a border vehicle search requires reasonable suspicion. United States v. Guzman-Padilla, 573 F.3d 865, 879 (9th Cir. 2009). The court looks to whether the search damaged the vehicle's safety of operability and if the search occurred in a particularly offensive manner *Id.* 

139. Flores-Montano, 541 U.S. at 154 n.2, 156.

140. See Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) (explaining how border searches can occur not only at the border entry itself but also at a "functional equivalent" or at an "extended" border).

141. See United States v. Caicedo-Guarnizo, 723 F.2d 1420, 1422 (9th Cir. 1984) (describing how the rationale of warrantless searches at international borders are assumed per se reasonable and the "extended border" doctrine is thus an expansion of this rule to ensure that borders remain secure).

142. See Extended Border Search and Probable Cause, Almeida-Sanchez v. United States, 413 U.S. 266 (1973), 1974 WASH. U. L. REV. 889, 889–94 (1973) (discussing the Almeida-Sanchez case and the concept of the extended border doctrine in connection to the case); see also Ralph V. Seep, Annotation, Validity of Warrantless Search Under Extended Border Doctrine, 102 A.L.R. Fed. 269 (1991) [hereinafter Validity of Warrantless Search] (outlining the general

individual's expectation of privacy because the individual, in theory, undergoes two searches. 143 One occurs at the border and one after entry into the country. 144 While travelers are put on notice for actual border searches, this expectation diminishes at "distant border equivalents [that] have no international status." 145 At distant checkpoints, no clear notice is given by border agencies or officials. 146 "Travelers who have not crossed the border thus cannot be thought to have given their implied consent to warrantless searches merely by traveling near the border." 147 If there is reasonable suspicion of the subject engaging in criminal activity, then courts consider these searches to be constitutional. 148 Law enforcement must also have "reasonable certainty" that the vehicle or contraband crossed the border. 149 Time and distance are part of the reasonable suspicion analysis in determining if a search

considerations in determining the validity of an extended border search, such as the border crossing itself, whether the search was delayed, and the presence of reasonable suspicion).

- 143. See Validity of Warrantless Search, supra note 142 (indicating that both United States v. Diaz-Segovia and United States v. Garcia are two instances where courts have recognized that the extended border search doctrine involves situations in which the search is delayed past the first practicable detention point within the United States).
- 144. See Santana, Almeida-Sanchez, supra note 123, at 238 n.149 (describing the implicit consent travelers provide when they cross a border zone).
  - 145. PS Rosenzweig, Functional Equivalent, supra note 122, at 1133.
- 146. See Gary N. Jacobs, Note, Border Searches and the Fourth Amendment, 77 YALE L.J. 1007, 1012 (1968) (setting forth the idea that "since the individual crossing a border is on notice that certain types of searches are likely to be made, his privacy is arguably less invaded by those searches").
- 147. PS Rosenzweig, Functional Equivalent, supra note 122, at 1133; see also Almeida-Sanchez, 413 U.S. at 281 (Powell, J., concurring) ("One who merely travels in regions near the borders of the country can hardly be thought to have submitted to inspections in exchange for a special prerequisite.").
- 148. See Validity of Warrantless Search, supra note 142 (providing cases from the Second, Third, Fourth, Fifth, Ninth, and Eleventh Circuits regarding this issue, while discussing how the level of suspicion rises for extended border searches further from the border).
- 149. See id. (distinguishing between an extended border search and an ordinary border search, which has a looser standard of suspicion since an "extended border search[] occur[s] after the actual entry into the country has occurred and intrude[s] more on an individual's normal expectation of privacy than regular border searches," but it is the "totality of the circumstances surrounding the search" that helps make this argument for reasonable suspicion away from the border after some lapse of time).

is constitutional and reasonable given the distance from the border. 150

### 3. Reasonable Suspicion, Time and Distance

Reasonable suspicion, in the border context, analyzes all facts given the situation to determine if border patrol agents violated an individual's privacy rights. <sup>151</sup> In *United States v. Alfonso*, <sup>152</sup> the Ninth Circuit determined that border agents met the reasonable suspicion requirement. <sup>153</sup> After arriving in the Los Angeles Harbor, border agents searched a ship, the *Santa Marta*, a second time within a day and a half of arrival. <sup>154</sup> The Court found reasonable suspicion to exist because of the "information known to the search party in this case, including the informant's tip, their own observations, and the arrests and seizure of cocaine from persons leaving the ship." <sup>155</sup>

In contrast, the Fifth Circuit found no reasonable suspicion in *United States v. Rangel-Portillo*. <sup>156</sup> Border patrol agents detained

<sup>150.</sup> See United States v. Caicedo-Guarnizo, 723 F.2d 1420, 1422 (9th Cir. 1984) (commenting on how the "validity of such a search [after a border crossing] depends on whether the fact finder, viewing the totality of the circumstances, is reasonably certain that the suspected smuggler did not acquire the contraband after crossing the border").

<sup>151.</sup> See id. (evaluating reasonable suspicion after a border crossing); see also United States v. Arvizu, 534 U.S. 266, 266–67 (2002) (remanding the appellate court's decision because in "making reasonable-suspicion determinations, reviewing courts 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," which "allows officers to draw on their own experiences and specialized training to make inferences from and deductions about the cumulative information available").

<sup>152.</sup> United States v. Alfonso, 759 F.2d 728, 728 (9th Cir. 1985).

<sup>153.</sup> See id. (affirming the search of a Colombian vessel in the Los Angeles harbor as a justified extended border search because it was supported by reasonable suspicion).

<sup>154.</sup> See id. at 734 (noting that it "is immaterial whether the situs be called the functional equivalent of the border, or the border itself," instead recognizing "that time and place are relevant, since the level of suspicion for extended border searches is stricter than the standard for ordinary border searches").

<sup>155.</sup> Id. at 738.

<sup>156.</sup> See United States v. Rangel-Partillo, 586 F.3d 376, 376 (5th Cir. 2009) (finding that the totality of the circumstances did not justify the agent to stop and search the defendant's vehicle because the reasonable suspicion standard was not

the vehicle about 500 yards from the border.<sup>157</sup> While the distance to the border factors into the court's Fourth Amendment analysis and afforded great weight, distance alone does not "constitute reasonable suspicion to stop and search an individual's vehicle."<sup>158</sup> The "[c]ourt [decided that it could not] conclude that an agent has reasonable suspicion to conduct a stop anytime an individual is sweating while riding in a vehicle in close proximity to this nation's southern border," without more.<sup>159</sup>

Federal law specifically provides authorized personnel, any officer or employee of the United States, at the border the authority to board, search, stop, and examine vehicles and persons with reasonable suspicion. <sup>160</sup> In addition, federal statute provides CBP officials with the authority to stop and search vessels or other vehicles anywhere within "a reasonable distance from any external boundary of the United States." <sup>161</sup> The Code of Federal Regulations defines "reasonable distance" to "mean within 100 air miles from any external boundary of the United States or any shorter distance that may be fixed by the chief patrol agent for CBP, or the special agent in charge for ICE." <sup>162</sup> To put it into perspective, according to

adequately met and decided that the defendant's motion to suppress evidence "obtained as the result of an allegedly unconstitutional stop by a United States Border Patrol agent . . . charg[ing] that he unlawfully transported undocumented aliens," should have been granted).

- 157. Id. at 380–81.
- 158. See id. (noting that there are various other factors to assess to evaluate if reasonable suspicion is met, aside from looking at the proximity to the border, which was the only factor evaluated in the present case).
- 159. See id. at 382 (concluding that the "overwhelming absence of any of these additional factors," led the court to not rationally find reasonable suspicion in this instance).
- 160. See 19 U.S.C. § 482 (2018) (allowing "officers or persons authorized to board or search vessels" including "any vehicle, beast, or person, on which or whom he or they shall suspect there is a merchandise which is subject to duty, or . . . contrary to law").
- 161. See 8 U.S.C. § 1357(a)(3) (2018) (breaking down the powers of immigration officers and employees without a warrant); see also Customs and Border Protection's (CBP'S) 100-Mile Rule, ACLU, https://www.aclu.org/sites/default/files/assets/13\_08\_01\_aclu\_100\_mile\_cbp\_zone \_final.pdf (last visited Oct. 15, 2019) (analyzing CBP's authority given the limited statutory guidance on the 100-Mile Rule, which has resulted in a degree of extra-constitutional powers for the Agency to authorize searches and seizures) [perma.cc/7VE5-NYBH].
- 162.~ See 8 C.F.R. § 287.1(b) (2018) (defining "reasonable distance" based on its use in The Immigration Reform and Control Act of 1986 to be within 100 miles

the 2010 census, about "[t]wo thirds of the U.S. population, or about 200 million people, reside within this expanded border region." <sup>163</sup>

The extended border defined by these statutes and regulations provides an expansive range of authority to border officials. For instance, the Ninth Circuit upheld extended border searches for searches from seven hours and 105 miles from the border, <sup>164</sup> up to fifteen hours and twenty miles from the border. <sup>165</sup> The Fifth Circuit similarly upheld an extended border search that was 150 miles from the border and 142 hours after a border crossing. <sup>166</sup> This included an instance where customs agents accidentally allowed a car to pass through the border into the United States without initially following it. <sup>167</sup> Instead, border officials located the car about thirty-five minutes later. <sup>168</sup> The Fifth Circuit disregarded the thirty-five minute interval where no surveillance occurred. <sup>169</sup> It concluded the interval to be "too brief to have been of any

or any shorter distance).

163. See Know Your Rights 100 Mile Border Zone, ACLU (2019), https://www.aclu.org/know-your-rights/border-zone/ (last visited Oct. 22, 2019) (giving a brief breakdown of the Fourth Amendment and the federal government's ability to conduct warrantless stops within 100 miles of the U.S. border for different scenarios) [perma.cc/A2FN-VUY8].

164. See Castillo-Garcia v. United States, 424 F.2d 482, 482–84 (9th Cir. 1970) (concluding that while the search of the vehicle occurred 105 miles from the border, the fact that there was "constant surveillance after the border crossing until the search, and there had been a change of drivers," the possibility that the 165 pounds of marijuana being placed after the crossing was obviated and the search was thus lawful).

165. See Rodriguez-Gonzalez v. United States, 378 F.2d 256, 256–59 (9th Cir. 1967) (affirming the lower court's decision that a valid border search occurred because while there was a change in drivers after crossing the border, the information provided by an informant gave the customs officials reasonable suspicion that the defendants may have been carrying marijuana).

166. See United States v. Martinez, 481 F.2d 214, 217 (5th Cir. 1973) (affirming the lower court's decision that the "search and seizure which yielded [a] truck of marijuana [to be] within the 'border search' exception to the Fourth Amendment").

167. See id. (mentioning how initially border agents accidentally let them through the border without following the vehicle).

168. See id. at 219 (determining reasonable suspicion trumped the thirty-five-minute interval).

169. See id. (qualifying their decision by noting that there was no reason for customs officials to doubt their original suspicions and constant surveillance of the vehicle took place after this initial thirty-five-minute period).

consequence," and held that the reasonableness standard would not be substituted with a per se rule based on the number of miles traveled inland and hours after entry into the country. 170

While significant weight is given to law enforcement at the border under these factors, the Ninth Circuit held that the extended Border Search Doctrine did not apply in *United States v. Cotterman.*<sup>171</sup> Border agents stopped Cotterman and his wife at the Mexican border after the Treasury Enforcement Communication System (TECS) returned a hit for Cotterman.<sup>172</sup> The hit indicated that Cotterman was on the sex offender registry and that he was potentially involved in child sex tourism.<sup>173</sup> The agents searched the vehicle and retrieved two laptops and three digital cameras.<sup>174</sup> After inspecting the electronic devices, the officer found several family photos along with several password-protected files.<sup>175</sup> The agents allowed the Cottermans to leave the border but retained the laptops and digital cameras.<sup>176</sup> The special agent then drove almost 170 miles from the border point to Arizona to deliver the electronic devices to an ICE agent.<sup>177</sup>

After determining that no contraband existed on the digital cameras and releasing the devices to the Cottermans, the ICE agent used forensic software to find seventy-five images of child pornography on the unallocated space in Cotterman's laptop. <sup>178</sup> When ICE opened the password-protected files, they obtained nearly 400 images of child pornography. <sup>179</sup>

The court determined that "[a] border search of a computer is not transformed into an extended border search simply because the device is transported and examined beyond the border." <sup>180</sup> Because

<sup>170.</sup> See id. (concluding that the border search exception applied, and no search occurred).

<sup>171.</sup> United States v. Cotterman, 709 F.3d 952, 961–62 (9th Cir.) (en banc), cert. denied, 571 U.S. 1156 (2014).

<sup>172.</sup> Id. at 957.

<sup>173.</sup> Id.

<sup>174.</sup> Id.

<sup>175.</sup> *Id.* at 957–58.

<sup>176.</sup> Id. at 958.

<sup>177.</sup> Id.

<sup>178.</sup> *Id*.

<sup>179.</sup> Id. at 958-59.

<sup>180.</sup> Id. at 961.

the case involved "a search initiated at the actual border and does not encounter any difficulties surrounding identification of a 'functional border," the court confined the analysis to situations where, "an attenuation in the time or location of conducting a search reflects that the subject has regained an expectation of privacy." Here, "Cotterman never regained possession of his laptop, [and] the fact that the forensic examination occurred away from the border . . . did not heighten the interference with his privacy." Time and distance apply "only after the subject or items searched have entered" the United States. Because "Cotterman's computer never cleared customs [and] entry was never effected," the extended border search doctrine did not apply. 184

Cotterman showcases a grey area in determining when an individual regains a heightened expectation of privacy at and near the border. Cotterman thus highlights the juncture between "classic" Fourth Amendment jurisprudence and the Border Search Doctrine, and the difficulties in delineating a clear line between the two concepts. Reasonable suspicion along with time and distance help to determine if a search is constitutional under the Border Search Doctrine. The analysis however is not clear-cut, and the existence of border policies poses another complicated layer for courts to analyze because of the lack of transparency and the possible breadth of interpretation.

#### 4. Border Search Policies Known to Date

DHS and CBP publish specific border policies and regulations to set certain parameters and highlight governmental authority. 188

<sup>181.</sup> *Id.* at 961–62.

<sup>182.</sup> Id. at 962.

<sup>183.</sup> *Id*.

<sup>184.</sup> *Id*.

<sup>185.</sup> Id. at 961–62.

<sup>186.</sup> See supra text accompanying notes 171–184.

<sup>187.</sup> See supra text accompanying notes 151–170.

<sup>188.</sup> See Border Security, U.S. Customs & Border Prot., https://www.cbp.gov/border-security (last updated Feb. 5, 2020) (last visited Sept. 27, 2020) (explaining CBP's mission at the border) [perma.cc/UCG2-3RZ6].

The CBP updated its policy (CBP Border Policy) on border searches of electronic devices on January 4, 2018. Before this, CBP's previous policy allowed for border agents to search a traveler's electronic devices without having to show any suspicion of any wrongdoing. Interest groups such as the EFF heavily criticized this old policy.

The new policy, however, purportedly differentiates between a "basic" search and an "advanced" one. 192 Basic searches are those not deemed "advanced." 193 It may be conducted with or without suspicion, where the officer may "examine an electronic device and may review and analyze information encountered at the border." 194 An advanced search on the other hand, involves the officer utilizing external equipment, "through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to

<sup>189.</sup> See U.S. Customs and Border Protection, Border Search of Electronic Devices, DEP'T OF HOMELAND SEC. (Jan. 4, 2018), https://www.dhs.gov/sites/default/files/publications/CBP%20Directive%203340-049A\_Border-Search-of-Electronic-Media.pdf (last visited Oct. 29, 2019) [hereinafter U.S. Customs and Border Protection 2018] (outlining the "guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets . . . and any other communication, electronic, or digital devices subject to inbound and outbound border searches by U.S. Customs and Border Protection (CBP)") [perma.cc/G2PT-WGFJ].

<sup>190.</sup> See U.S. Dep't of Homeland Sec., Private Impact Assessment for the Border Searches of Electronic Devices, DEP'T OF HOMELAND SEC. (Aug. 25, 2009), https://www.dhs.gov/sites/default/files/publications/privacy\_pia\_cbp\_laptop.pdf (last visited Jan. 19, 2020) [hereinafter DHS, Searches of Electronic Devices] (discussing the legal foundation for the border search exception while distinguishing between the privacy interests between electronic devices as opposed to traditional items found at the border, such as a briefcase or a backpack) [perma.cc/PGT5-DX9P].

<sup>191.</sup> See Sophia Cope & Aaron Mackey, New CBP Border Device Search Policy Still Permits Unconstitutional Searches, ELEC. FRONTIER FOUND. (Jan. 8, 2018), https://www.eff.org/deeplinks/2018/01/new-cbp-border-device-search-policy-still-permits-unconstitutional-searches (last visited Jan. 19, 2020) (comparing the new policy against the old policy to analyze the potential loopholes and vague language, which could lead to violations to travelers' constitutional rights) [perma.cc/5AV4-LTT2].

<sup>192.</sup> See U.S. Customs and Border Protection 2018, supra note 189 (explaining the different procedures taken at the border depending on whether the search is basic or advanced for electronic devices held at the border).

<sup>193.</sup> *Id*.

<sup>194.</sup> *Id*.

review, copy, and/or analyze its contents."<sup>195</sup> Either reasonable suspicion or the presence of a "national security concern" permits an advanced search.<sup>196</sup>

The policy provides some examples, but no formal definition in the text describes what constitutes a "national security concern." An individual can remain present during the search, unless "there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present." "Travelers [have an obligation] to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents." <sup>199</sup> While officers retrieve or access remotely stored information on a device, they must disable network connectivity, i.e. turn on airplane mode. <sup>200</sup> This policy will not be reviewed again until January of 2021. <sup>201</sup>

In 2019, Judge Casper of the United States District Court for the District of Massachusetts concluded that no distinction exists between manual and forensic device searches, as dictated by other

<sup>195.</sup> *Id*.

<sup>196.</sup> See id. (noting that the new policy requires supervisory approval by a Grade 14 level or higher for an advanced search of an electronic device by an officer and examples of a national security concern include, "existence of a relevant national security-related lookout combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list").

<sup>197.</sup> See U.S. Customs and Border Protection 2018, supra note 189 (describing how all searches are ultimately documented in the appropriate CBP systems, and if a supervisor is not available to be present during the search, then the examining Officer is required to notify the appropriate supervisor of the results as soon as possible).

<sup>198.</sup> See id. (emphasizing that this permission does not mean that the individual is allowed to observe the search itself because of the possibility of revealing "law enforcement techniques or potentially compromis[ing] other operational considerations").

<sup>199.</sup> *Id*.

<sup>200.</sup> See id. (providing that the easiest way is to place the device in airplane mode to avoid violating privacy issues in this regard).

<sup>201.</sup> Id.

courts.<sup>202</sup> In *Alasaad v. McAleenan*,<sup>203</sup> the court found that international travelers have a significant privacy interest in their digital data at the border.<sup>204</sup> The case began as a constitutional challenge to the policies regarding search and seizures of electronic devices at the border.<sup>205</sup> Yet, it ended when the court ruled that suspicionless electronic device searches at the border violate the Fourth Amendment.<sup>206</sup>

The court decided that both types of searches now require reasonable suspicion instead of probable cause. <sup>207</sup> The court did not find a meaningful distinction between the two types of searches. Consequently, the distinction between a "basic" and an "advanced" search provided in the CBP guidelines no longer exists under this determination. <sup>208</sup> Instead, the decision "declare[d] that the CBP and ICE policies for 'basic' and 'advanced' searches, as presently defined, violate the Fourth Amendment to the extent that the policies do not require reasonable suspicion that the devices contain contraband." <sup>209</sup> This broad ruling encompasses not only U.S. citizens but international travelers as well and heightens concerns regarding privacy interests at the border. <sup>210</sup>

Border search agents or agents along the border consequently have a great deal of authority under the border search exception.<sup>211</sup>

<sup>202.</sup> See Memorandum and Order at 33–38, Alasaad v. McAleenan, No. 17-cv-11730-DJC (D. Mass. Nov. 12, 2019), ECF No. 109 [hereinafter Alasaad Order] (determining that reasonable suspicion rather than probable cause applied to both a basic and advanced search as described in CBP and ICE's border policies); see also United States v. Touset, 890 F.3d 1227, 1232, 1235 (11th Cir. 2018) (holding that "searches at the border of the country 'never require probable cause or warrant" because "the advent of sophisticated technological means for concealing contraband only heightens the need of the government to search property at the border unencumbered by judicial second-guessing").

<sup>203.</sup> Alasaad v. McAleenan, No. 17-cv-11730-DJC (D. Mass. Nov. 12, 2019).

<sup>204.</sup> See Alasaad Order, supra note 202, at 33–38 (holding that expungement of all information gathered from, or copies made of, contents of travelers' electronic devices during unconstitutional border searches was not warranted).

<sup>205.</sup> Id.

<sup>206.</sup> Id.

<sup>207.</sup> Id

<sup>208.</sup> See id. (deciding both searches require reasonable suspicion).

<sup>209.</sup> Id. at 46–47.

<sup>210.</sup> See id. (determining that searches going forward for electronic devices require reasonable suspicion prior to the search).

<sup>211.</sup> See United States v. Martinez, 481 F.2d 214, 218 (5th Cir. 1973) (noting

No matter the item searched, agents are given a great deal of latitude based on the precedent at hand. Despite the fact that government interests may be broader at the border, law enforcement must still show "the degree to which [the search exception] is needed for the promotion of legitimate government interests." This, however, does not mean that courts will allow suspicionless searches in every circumstance. 214

## III. The Tension Between the Fourth Amendment and the Border Search Doctrine

Technological advancement poses a problematic hurdle for the Fourth Amendment and the Border Search Doctrine. This next section highlights the growing tension between the two doctrines created by GPS tracking and the problematic new policies disclosed through *United States v. Ignjatov*.

#### A. GPS Tracking & Its Place in The Fourth Amendment

Flores-Montano ensures that a vehicle may be searched at the border with a limited amount of suspicion. However, the Supreme Court in Jones held that warrantless installation of a GPS on an individual's car violates the Fourth Amendment. A great degree of overlap between these two doctrines exists and may pose problematic consequences moving forward. United States v. Ignjatov highlights this overlap and challenge.

#### 1. United States v. Ignjatov

that "courts have long recognized that the border is an elastic concept, not susceptible to precise definition in temporal or spatial terms," which is necessary to allow for customs officials to adequately manage the border).

- 212. See supra notes 118-187 and accompanying text.
- 213. Riley v. California, 573 U.S. 373, 385 (2014).
- 214. See Alasaad Order, supra note 202, at 33–38 (noting that the government's differentiation between the two searches lacked reasonableness).
- 215. See United States v. Flores-Montano, 541 U.S. 149, 149 (2004) (holding that the search did not require reasonable suspicion).
  - 216. United States v. Jones, 565 U.S. 400, 400–01, 404–05, 411–12 (2012).

In *United States v. Ignjatov*, the Federal Bureau of Investigations (FBI) and the LAPD investigated a drug ring running from Toronto through Chicago to Southern California.<sup>217</sup> After seizing ten duffle bags containing cocaine from an individual named Karac, who entered into the United States in 2017 from Canada in a Bo-Mak truck, a confidential source revealed the possibility of another dry run in the near future.<sup>218</sup> On October 19, 2017, the CBP notified Special Agent Hanna Monroe that the defendants would enter the United States in a Bo-Mak truck, matching the one that Karac used in March.<sup>219</sup>

At the request of the FBI and the LAPD, a CBP officer placed two GPS tracking devices on the defendants' truck and trailer at the border on October 20, 2017. DHS agents also inspected the vehicles at the border but found nothing unusual. The there, FBI agents and LAPD tracked the vehicle on their computers for the next thirty-three hours as the truck made its way to Los Angeles. The government utilized a program called Covert Tracker to track the GPS devices. Agents could log on to the program at any location to verify the GPS data. The device not only recorded the historical location data, but it also recorded the

<sup>217.</sup> See Cyrus Farivar, Cheese Danish Shipping, Warrantless GPS Trackers, and a Border Doctrine Challenge, ARS TECHNICA (Sept. 2, 2018, 10:50 AM), https://arstechnica.com/tech-policy/2018/09/judge-to-feds-no-you-cant-warrantlessly-put-a-gps-device-on-truck-entering-us/ (last visited Sept. 22, 2020) [hereinafter Farivar, Cheese Danish] (reporting on the facts of United States v. Ignjatov, how LAPD and FBI knew of the individuals running the ring, the ultimate ruling handed down by Judge Bernal, and the implications of warrantless tracking permitted at the border) [perma.cc/8T8P-NRQ8]; see also Ignjatov Complaint, supra note 2, at 1–19 (laying out the allegations and background leading to the arrest).

<sup>218.</sup> See EFF Complaint, supra note 1, at 1 (outlining the details and reasoning for the filing of litigation, as well as referencing the problematic nature of Homeland Security's policies).

<sup>219</sup>. See Amended Order, supra note 12, at 2 (describing the facts of the case prior to ruling).

<sup>220.</sup> Id.

<sup>221.</sup> Id.

<sup>222.</sup> See Ignjatov Complaint, supra note 2, at 13-19 (documenting and describing the surveillance progress while tailing the vehicle).

<sup>223.</sup> See id. (noting the program is able to obtain a nearly exact address).

<sup>224.</sup> See id. (noting the program keeps all historic locational data which agents can see upon sign-in, as well as download the data to Excel).

speed of the vehicle.<sup>225</sup> The recording intervals were set for every fifteen minutes, but agents increased this as the defendants approached California.<sup>226</sup>

Physical surveillance of the truck did not begin until October 22 when the defendants drove from San Bernardino County to Los Angeles County. 227 When the defendants finally stopped near an airport, law enforcement officers approached and only found, "15 four-pound packages of sugar, cheese Danishes, numerous cell phones, and an empty duffle bag, which when sniffed by police dogs "alerted [the officers] to the presence of narcotics." LAPD released both men but arrested the defendants as they attempted to return to Canada for conspiracy to traffic cocaine. 229 The GPS trackers remained on the vehicles until their arrest. 230

The defendants argued that the government's warrantless installation and monitoring of their vehicles violated their Fourth Amendment rights.<sup>231</sup> Relying on *Jones*, the defendants argued that the warrantless use of a GPS is illegal when the installation amounts to a trespass, regardless of the fact that a "border search" and an "extended border search" are exceptions to the search warrant requirement.<sup>232</sup> The government, in turn, argued that the "installation and use of GPS devices were lawful [under the border search doctrine], and even if not, the evidence [was] admissible

<sup>225.</sup> Id.

<sup>226.</sup> Id.

<sup>227.</sup> Id.

<sup>228.</sup> See Farivar, Cheese Danish, supra note 217 (relaying the facts behind the arrest of the two defendants).

<sup>229</sup>. See id. (noting that both defendants were arrested in Port Huron, MI as they were returning to Canada).

<sup>230.</sup> See Ignjatov Complaint, supra note 2, at 13–19 (stating that special agents were monitoring defendants until their arrest on Oct. 28, 2017); see also Gruel Declaration, supra note 10, at 9 (highlighting that on Oct. 19, 2017, GPS tracking devices were applied to the truck).

<sup>231.</sup> See Joint Notice of Mot. and Mot. to Suppress Evidence by Defendants Ignjatov and Hristovski at 6, United States v. Ignjatov, No. 5:17-cr-00222-JGB, (C.D. Cal. May 11, 2018), ECF No. 86 (breaking down Fourth Amendment jurisprudence and why  $United\ States\ v.\ Jones\$ should apply).

<sup>232.</sup> See id. at 8–15 (arguing that border search exception should not apply because the GPS allows tracking away from the border, which did not fall under the extended border doctrine).

under the attenuation, inevitable discovery, and good faith exceptions to the exclusionary rule."<sup>233</sup>

The judge in *Ignjatov* ruled in favor of the defendants following *United States v. Jones*.<sup>234</sup> The court determined that "the key to determining whether the search required reasonable suspicion depend[ed] on the intrusiveness of the vehicle search."<sup>235</sup> The court found border vehicle search cases like *Flores-Montano* and subsequent Ninth Circuit cases focused on "whether the government's search resulted in physical damage or destruction to the vehicle at issue."<sup>236</sup> These vehicle search cases "all involved searches conducted and completed at the border, which [had] 'minimal or no impact beyond the search itself."<sup>237</sup> The court differentiated these cases from *Ignjatov* because it did not believe that "an analysis dependent on the physical aspects of the search is appropriate here where the search extends beyond the installation of the GPS device."<sup>238</sup>

Instead, the *Ignjatov* court delineated certain limitations to the border search doctrine.<sup>239</sup> In particular, the court concluded that "[o]nce the entity at issue is beyond the border, the concerns animating the border search doctrine, namely the integrity of the border, diminish, and the robust Fourth Amendment requirements adhere."<sup>240</sup> Installing the GPS device onto the vehicle, while not "akin to reading a diary line by line,"<sup>241</sup> exceeded the "scope of the

<sup>233.</sup> Amended Order, *supra* note 12, at 4; *see also* Gov't's Opposition to Defendants Slavco Ignjatov and Valentine Hristovski's Joint Mot. to Suppress Evidence at 10–25, United States v. Ignjatov, No. 5:17-cr-00222-JGB, (C.D. Cal. May 21, 2018), ECF No. 87 (arguing that the installation was lawful and supported by probable cause, and even if not, it is admissible under the attenuation and inevitable discovery exceptions and good faith exception).

<sup>234.</sup> See Amended Order, supra note 12, at 5–8, 15 (determining both the border search doctrine and extended border search doctrine did not apply).

<sup>235.</sup> *Id.* at 5.

<sup>236.</sup> Id. at 5–6.

<sup>237.</sup> Id. at 6.

<sup>238.</sup> Id.

<sup>239.</sup> See id. at 7 (differentiating between the extended border and the border itself to find that neither exception applied to the installation of the GPS device).

<sup>240.</sup> *Id*.

<sup>241.</sup> United States v. Cotterman, 709 F.3d 952, 961–62 (9th Cir.) (en banc), cert. denied, 571 U.S. 1156 (2014).

suspicionless searches authorized in the border vehicle cases."<sup>242</sup> This was because the installation of a GPS device "implicates a search away from the border, once the target has gained entry into the country.<sup>243</sup> Applying *Jones*, where the Supreme Court "defined the search as encompassing both the installation and use of the GPS,"<sup>244</sup> *Ignjatov* refused to extend the border search doctrine to a point beyond the border where a "precise comprehensive record of a person's public movements"<sup>245</sup> could be acquired.<sup>246</sup>

The *Ignjatov* court also determined that the installation of the GPS and the subsequent monitoring were not justified under the extended border search.<sup>247</sup> Relying on Justice Alito's concurrence in *Jones*,<sup>248</sup> the court determined that even though the electronic surveillance occurred for fewer than 48 hours, "it is this unceasing search over the period that precludes the application of the extended border search doctrine."<sup>249</sup> The court found extended border search cases to typically encompass a definitive search at some distance from the border, unlike here.<sup>250</sup> The search here differed significantly because the government agents tracked the defendants' truck and trailer for almost 48 hours, and "the Covert Tracker program obtained [the] Defendants' location information at regular intervals."<sup>251</sup> It also permitted government agents to

- 242. Amended Order, supra note 12, at 7.
- 243. Id.
- 244. Id.; United States v. Jones, 565 U.S. 400, 404-05, 411-12 (2012).
- 245. United States v. Jones, 565 U.S. at 415 (Sotomayor, J., concurring).
- 246. See Amended Order, supra note 12, at 7 (discussing the ramifications of an extension of the border search doctrine).
- 247. See id. at 8 (finding that the tracking utilized in *Ignjatov* to be "poles apart" from discrete searches under the extended border search doctrine and thus not an exception).
- 248. See Jones, 565 U.S. at 420 (Alito, J., concurring) (discussing how a search occurred prior to the four-week mark in Jones).
  - 249. Amended Order, supra note 12, at 8.
- 250. See id. (finding the search in *Ignjatov* to go beyond the searches as those under the extended border doctrine); see also Rodriguez-Gonzalez v. United States, 378 F.2d 256, 258 (9th Cir. 1967) (noting that to determine whether a search is legal when it is not at the immediate border, a court must look at the totality of the circumstances, which includes time and distance); see also United States v. Guzman-Padilla, 573 F.3d 865, 877–78 (9th Cir. 2009) (emphasizing that border searches can occur at a "functional border" with no suspicion as long as they are not "unreasonably intrusive").
  - 251. Amended Order, supra note 12, at 8.

download all of the historic data recorded from any device at any time. This type of tracking is poles apart from the discrete searches conducted under the extended border search doctrine. The court accordingly concluded that the search of the truck along with the installation of the GPS device did not classify as an extended border search.

# B. Unknown Policies & Ongoing Electronic Frontier Foundation Suit

While the court in *Ignjatov* applied the *Jones* intrusion test to grant the defendants' motion to suppress, it also addressed how the border search doctrine fared post *Jones* and effectively limited the government's authority in this domain.<sup>255</sup>

The government argued and submitted declarations stating that DHS's policy allowed for "customs officers [to] install a GPS tracking device on a vehicle at the United States border without a warrant or individualized suspicion." Moreover, "[Homeland Security Investigation (HSI)] limit[ed] warrantless GPS monitoring to 48 hours, with the exception of airplanes, commercial vehicles, and semi-tractor trailers, which have a significantly reduced expectation of privacy in the location of their vehicles." The declaration suggested that DHS believed HSI's position and policy to be "consistent with the U.S. Supreme Court's decision in . . . Jones . . . [and] Flores-Montano . . . ." Assistant Director Matthew C. Allen finished his declaration by indicating

<sup>252.</sup> See id. (discussing the tracking program utilized by border officials during the surveillance).

<sup>253.</sup> *Id*.

<sup>254.</sup> See id. (determining that based on the totality of circumstances, the installation could not be classified as an extended border search).

<sup>255.</sup> See id. ("Therefore, this Court is hesitant to mechanically apply the border search doctrine where the search stretches far beyond the conduct at the border . . . .").

<sup>256.</sup> See Allen Declaration, supra note 17, at 1–3 (providing a formal statement as the "Assistant Director (AD) for the Domestic Operations Division within the U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI)").

<sup>257.</sup> Id.

<sup>258.</sup> Id.

that "HSI's position on the use of GPS tracking devices were [sic] developed in consultation with the Department of Justice, in response to the 2012 *Jones* decision, and is found in HSI policies and procedures," including "trainings regularly provided to HSI personnel."<sup>259</sup> No further mention of these policies occurred during discovery.<sup>260</sup> A lack of transparency regarding these policies and procedures can result in inconsistent applications and enforcement measures by law enforcement at the border, which can lead to an imbalance in privacy expectations by citizenry.<sup>261</sup>

Since this decision, the EFF brought suit against DHS to learn more about these policies and procedures. The suit is ongoing, but it came after the Electronic Frontier Foundation submitted a FOIA request to ICE for "records pertaining to the agency's policies and procedures regarding the use of GPS tracking devices at the U.S. border." 263

The request sought two types of information: "(1) Policies and/or procedures regarding the use of the GPS tracking devices on vehicles crossing the border; and (2) Training manuals and/or training materials on the use of GPS tracking devices on vehicles crossing the border."264 ICE sent a response on March 11, 2019, indicating that a search through ICE's HSI produced three pages of relevant materials; however, "all three pages would be withheld under Exemption 7(E)."265 Exemption 7(E) affords law enforcement agencies the ability to deny a request for information that would "disclose techniques and procedures...or would disclose guidelines for law enforcement investigations

<sup>259.</sup> Id

<sup>260.</sup> See Amended Order, supra note 12, at 8 (discussing the policy's specifics known at the time).

<sup>261.</sup> See Gruel Declaration, supra note 10, at 2 (describing how in his sixteen years as an AUSA and ten years as Chief of the General Crimes Section, he has never heard of "a border exception permitting the warrantless installation of a GPS tracking device or some sort of 48 hour-rule," even after asking several other agents, no one "had heard of this '48 hour rule' or the 'commercial vehicle exception").

<sup>262.</sup> See EFF Complaint, *supra* note 1, at 1 (highlighting the problematic practices unknown to the general public and the impasse currently in place while DHS and CBP refuse to comply and fulfill EFF's FOIA request).

<sup>263.</sup> *Id*.

<sup>264.</sup> Id. at 3-4.

<sup>265.</sup> Id. at 4.

procedures...[that] could reasonably be expected to risk circumvention of the law."266 EFF filed an administrative appeal shortly afterwards to challenge the withholding of records and the adequacy of ICE's search for records. 267 ICE has since conducted supplemental searches and four "productions." <sup>268</sup> ICE processed 521 pages of material, withholding some information pursuant to an Exemption, on December 30, 2019. 269 ICE then processed 1,091 pages of potentially responsive material on March 5, 2020, but only produced ninety-four pages because the others were deemed non-responsive.<sup>270</sup> On May 5, 2020, ICE provided EFF "with a cover letter stating that ICE had processed 577 pages of material and zero pages were responsive to [EFF's] FOIA request."271 Finally, on July 6, 2020, ICE made its final interim production to EFF's FOIA request, producing 361 pages as responsive, even though it processed 576 pages.272 ICE provided no other information regarding these documents.<sup>273</sup> Similarly, CBP has since conducted a supplemental search to EFF's original request, and returned approximately forty-nine records.<sup>274</sup> However, after reviewing for responsiveness, CBP reported on April 1, 2020 that forty-seven records were nonresponsive, and one record was withheld under an Exemption.<sup>275</sup> CBP provided no other

<sup>266.</sup> Department of Justice Guide to the Freedom of Information Act Exemption 7(E), U.S. DEP'T OF JUST., https://www.justice.gov/oip/foia-guide/exemption\_7\_e/download (last visited Feb. 4, 2020) [hereinafter Exemption 7(E)] (describing how Exemption 7(E) affords protection to law enforcement information that "could reasonably be expected to risk circumvention of the law") [perma.cc/4KQB-TT5L].

<sup>267.</sup> See EFF Complaint, supra note 1, at 4 (arguing that ICE had failed to provide details as to why the records risked circumvention of the law).

<sup>268.</sup> See Joint Status Report at 1–2, Elec. Frontier Found. v. Dep't of Homeland Sec., No. 1:19-cv-02578 (D.C.C. July 6, 2020), ECF No. 12 (highlighting the requests and productions to date and requesting for the litigation to proceed to cross-motions of summary judgment).

<sup>269.</sup> See id. (stating ICE withheld materials due to Exemptions 5, 6, 7(C) and 7(E)).

<sup>270.</sup> See id. at 2. (noting that the second interim response also withheld materials under FOIA Exemptions 5, 6, 7(C) and 7(E)).

<sup>271.</sup> *Id*.

<sup>272.</sup> Id.

<sup>273.</sup> Id. at 1-3.

<sup>274.</sup> Id. at 3.

<sup>275.</sup> Id.

information regarding these documents, and only referred one document to ICE for processing.<sup>276</sup>

As of Aug. 6, 2020, both parties submitted status reports but await resolution in the overall suit. <sup>277</sup> Given this, knowledge of CBP and DHS policies regarding GPS tracking at the border remain limited to the Declarations filed in *Ignjatov*. <sup>278</sup> Without further information, these policies remain vague and ambiguous given Fourth Amendment precedent to date. Transparency keeps individuals and agencies accountable for their actions by providing notice and consent. Without fully understanding the reasoning and authority for these policies and procedures, violations to privacy will continue if left unchecked. Given the problematic nature of these policies if left unchecked, the next section addresses these policies, given the limited facts known to date, and their place in Fourth Amendment jurisprudence.

#### IV. GPS Devices & Current Border Policies

Fourth Amendment precedent, while evolving, remains stagnant and burdened by the advancements of technology.<sup>279</sup> Courts grapple with changing technologies while remaining faithful to *Katz*'s reasonable expectation of privacy test and the common law of trespass.<sup>280</sup> At the same time, the Border Search Doctrine remains steadfast in granting law enforcement officers with an expansive degree of authority to protect national interests.<sup>281</sup> This section highlights the overlapping and competing nature of the two doctrines, while evaluating where a GPS tracking device should fall on this spectrum given precedent and policies known to date.

<sup>276.</sup> Id.

<sup>277.</sup> EFF Order, supra note 22.

<sup>278.</sup> Asatur Declaration, supra note 5, at 2–4; Monroe Declaration, supra note 9, at 5–8; Gruel Declaration, supra note 10, at 1–9; Allen Declaration, supra note 17, at 1–3.

<sup>279.</sup> See discussion supra Sections II.A-B, III.A-B.

<sup>280.</sup> See discussion supra Section II.A.

<sup>281.</sup> See discussion supra Section II.B.

## A. Classic Fourth Amendment Interpretation

If a court analyzes the installation of a GPS tracking device and subsequent electronic monitoring at the border solely under "classic" Fourth Amendment precedent, then a court should  $_{
m the}$ installation and surveillance unconstitutional search, similar to Jones and Carpenter.<sup>282</sup> The Supreme Court in Jones determined that the nature of the intrusion determined the unconstitutionality rather than Katz's reasonable expectation of privacy.<sup>283</sup> It found the installation of a GPS device without a warrant, regardless of the duration used for tracking, to violate the Fourth Amendment. 284 The Supreme Court in Carpenter then found locational privacy to exist and determined that extensive tracking of an individual violates the Fourth Amendment.<sup>285</sup> If applied directly to the border context, then the physical intrusion and violation of privacy from the installation and surveillance using a GPS tracking device follows the same logic. 286 Even if courts determine that the installation at the border is not a violation under *Jones*, Carpenter should still apply and constitute a search under the Fourth Amendment.<sup>287</sup> Even though Carpenter draws the line at seven days for CSLI data, a court will likely find locational privacy violated before this threshold, thus finding the installation and surveillance to be an unconstitutional

<sup>282.</sup> See United States v. Jones, 565 U.S. 400, 401–03, 408–12 (2012) (concluding that intruding on an individual's property is a search); see also Carpenter v. United States, 138 S. Ct. 2206, 2217–19 (2018) (determining that obtaining seven days of CSLI was a search).

 $<sup>283. \;\;</sup>$  See Jones, 565 U.S. at 404, 408–12 (holding the GPS installation to be a search).

<sup>284.</sup> See id. (holding the GPS tracker violated the Fourth Amendment due do the trespass that had to have occurred in order to install the device).

<sup>285.</sup> See Carpenter, 138 S. Ct. at 2210, 2217–19 (maintaining the idea that individuals have a reasonable expectation of privacy in the whole of their movements).

<sup>286.</sup> See supra notes 283–285 and accompanying text.

<sup>287.</sup> See Carpenter, 138 S. Ct. at 2210, 2217–19 (determining that a person has a right to their locational privacy).

search.<sup>288</sup> Jones and Carpenter are binding precedents, and therefore, lower courts must follow them.<sup>289</sup>

This analysis, however, complicates under the Border Search Doctrine.

# B. Applying the Border Search Doctrine

Even though the district court judge in *Ignjatov* determined that it was unconstitutional to install a GPS monitoring device to Ignjatov's vehicle under *Jones*, a few problems remain.<sup>290</sup> First, the brief disclosure of DHS and CBP's border policy highlights an incongruity between Fourth Amendment precedent and what enforcement agencies deem permissible under the Border Search Doctrine.<sup>291</sup> Second, *Ignjatov* illustrates the growing tension between "classic" Fourth Amendment Supreme Court doctrine and the Border Search Doctrine as a whole.<sup>292</sup> Consequently, it is necessary to determine whether a GPS monitoring device falls under the Border Search Doctrine, the Fourth Amendment, or a combination of the two.

An analysis under the Border Search Doctrine requires a multi-level inquiry, focusing on the type of search, the location of the search and the border policies to date, as well as Fourth

<sup>288.</sup> See id. (holding that when the Government accessed CLSI data from wireless carriers, it invaded the defendant's reasonable expectation of privacy); see also Amended Order, supra note 12, at 1–8 (determining that the GPS tracking and surveillance utilized to constitute a search under the Fourth Amendment).

<sup>289.</sup> See John M. Walker, Jr., The Role of Precedent in the United States: How Do Precedents Lose Their Binding Effect?, STAN. LAW SCH. CHINA GUIDING CASES PROJECT (Feb. 29, 2016), https://cgc.law.stanford.edu/wp-content/uploads/sites/2/2016/02/CGCP-English-Commentary-15-Judge-Walker.pdf (last visited Jan. 19, 2020) (discussing stare decisis and its effect on the judicial system) [perma.cc/9LC9-DCCB].

<sup>290.</sup> See Amended Order, supra note 12, at 4–8 (granting defendants' motion to suppress).

<sup>291.</sup> See Allen Declaration, supra note 17, at 2–3 (mentioning the policy purportedly being in line with the Border Search Doctrine, Jones, and Flores-Montano); see also discussion supra Part II.

<sup>292.</sup> See Amended Order, supra note 12, at 1–8 (analyzing the GPS device under the Border Search Doctrine and "classic" Fourth Amendment principles to determine that the GPS tracking and surveillance to not be an exception under the Border Search Doctrine).

Amendment principles. An evaluation of the installation of a GPS device and subsequent monitoring in each context follows.

## 1. GPS device in a Routine v. Non-Routine Context

If a court evaluates the installation of a GPS tracking device at the border and its subsequent surveillance, then the Border Search Doctrine should not allow for officials to "conduct suspicionless inspections at the border" based on Jones<sup>293</sup> and Carpenter.<sup>294</sup> Jones concluded that the "Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search." The Jones Court, however, did not evaluate the duration of the tracking but rather looked at the intrusion.<sup>296</sup> Five Justices argued in Carpenter that locational privacy existed as mentioned in *Jones*, determining that an individual maintains a "legitimate expectation of privacy in the record of his movements . . . [through his] location information."297 Additionally, Carpenter explicitly determined that obtaining seven days of location information by tracking an individual violates the Fourth Amendment.<sup>298</sup> The Court mentions in the holding that CSLI is more intrusive than GPS tracking.<sup>299</sup> A connection between CSLI and GPS tracking is therefore possible.<sup>300</sup> Taken together, a search, in the GPS context at the border, needs to be separated out first by the installation and then by the subsequent tracking.<sup>301</sup>

 $<sup>293.\</sup> See$  United States v. Jones, 565 U.S. 400, 404–05, 411–12 (2012) (concluding the installation to trespass on property).

<sup>294.</sup> See Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (deciding the location information obtained was a search).

<sup>295.</sup> Jones, 565 U.S. at 404.

<sup>296.</sup> See id. at 405–11 (discussing why the trespass on property implicated a search).

<sup>297.</sup> See Carpenter, 138 S. Ct at 2213–20 (highlighting why surveillance is detrimental).

 $<sup>298.\</sup> See\ id.$  at 2217-19 (determining CSLI obtained extended beyond expectations of privacy).

<sup>299.</sup> See id. at 2218 (explaining that CSLI poses "greater privacy concerns than the GPS monitoring . . . in Jones").

<sup>300.</sup> See supra notes 293, 297–298 and accompanying text.

<sup>301.</sup> See infra notes 302-358 and accompanying text.

Based on *Flores-Montano*, no balancing test is applicable and the differentiation between a "routine" and "non-routine" search is irrelevant for vehicle searches at the border. 302 This, however, should not be applicable to the installation of the tracking device and subsequent monitoring.<sup>303</sup> Unlike the disassembly of a fuel tank at the border, the installation of a tracking device is more intrusive and does not conclude at the border.<sup>304</sup> While both may be based on a degree of suspicion of some sort, one focuses on finding tangible evidence of wrongdoing, such as contraband, at the border.<sup>305</sup> On the other hand, the installation focuses on the accumulation of informational data, regardless of the tangible evidence located in the vehicle at the time of crossing the border.<sup>306</sup> The vehicle search in Flores-Montano commenced and ceased at the border.<sup>307</sup> The installation of a GPS tracking device is more intrusive than the disassembly of a fuel tank because notice and consent are given for the latter while none is given for the

<sup>302.</sup> See United States v. Flores-Montano, 541 U.S. 149, 149 (2004) (finding greater government interests in the vehicular context and thus no reasonable suspicion is required for vehicular searches).

<sup>303.</sup> See Amended Order, supra note 12, at 1–8 (concluding that GPS installation and monitoring is an extensive search and not one solely rooted at the border).

<sup>304.</sup> See id. (determining that the use of the tracking program provided instantaneous data).

<sup>305.</sup> See Flores-Montano, 541 U.S. at 149 (highlighting how Congress grants executive plenary authority for routine searches at the border to not only regulate border duties but to prevent contraband from entering into this country); see also United States v. Caicedo-Guarnizo, 723 F.2d 1420, 1422 (9th Cir. 1984) (pointing out that the validity of a search depends on the totality of the circumstances and being reasonably certain that contraband was acquired after crossing the border).

<sup>306.</sup> See Amended Order, supra note 12, at 7 (concluding that "data collection inherent in GPS monitoring exceeds the scope of the suspicionless searches authorized in the border vehicle cases" and that the "placement of a GPS device at the border necessarily implicates a search away from the border, once the target has gained entry into the country"); see also United States v. Jones, 565 U.S. 400, 420 (2012) (Alito, J., concurring) (defining the search to be both the installation and use of the GPS device, instead of separating out the two procedures); see also Ignjatov Complaint, supra note 2, at 1–13 (noting how the initial search did not turn up any contraband and law enforcement utilized it as an opportunity to attach the GPS tracking devices).

<sup>307.</sup> See Amended Order, supra note 12, at 7 (emphasizing that the "surreptitious surveillance of an individual's movements through placement of a GPS device on a vehicle implicates far greater privacy concerns than the physical integrity of the vehicle, and extends beyond the permissible scope of a border search").

former.<sup>308</sup> An individual can reasonably expect to be searched at a point where he enters into the country; however, it is the manner in which law enforcement conducts the search that makes the GPS installation more intrusive.<sup>309</sup> While the disassembly is complete at the border, the installation is only the beginning of the search in question and can continue for an indefinite period of time.<sup>310</sup> Even though the Border Search Doctrine provides tremendous latitude to border officials to protect the international border, the installation and subsequent monitoring extend beyond a simple search at the border in question.<sup>311</sup> Therefore, the GPS tracking device should not be considered merely in the vehicular context at the border.

Flores-Montano also mentions instances where "some searches of property are so destructive" or "particularly offensive," to require particularized suspicion.<sup>312</sup> The definition of an "offensive" search remains an open question for courts.<sup>313</sup> Because this Note focuses on installation of a GPS device and the subsequent tracking, which creates limited-to-no damage to a vehicle's safety or operability due to installation and placement practices to date,<sup>314</sup> no further analysis of Flores-Montano follows.

<sup>308.</sup> See Santana, Almeida-Sanchez, supra note 123, at 238 n.149 and accompanying text; see also Amended Order, supra note 12, at 7 (discussing how a GPS goes beyond the border search's permissible scope); see also Flores-Montano, 541 U.S. at 149 (reiterating that "this Court has long recognized that automobiles seeking entry into this country may be searched," so the defendant did not have possessory interest in his gas tank which is a piece of the automobile itself). If no consent is given to take apart the fuel tank, given the fact that the disassembly takes place at the border, this differentiates the disassembly from the installation and subsequent surveillance using a GPS tracking device because an individual's expectation of privacy heightens as he or she leaves the border. Border Searches and the Fourth Amendment, supra note 146, at 1012.

<sup>309.</sup> See Santana, Almeida-Sanchez, supra note 123, at 238 n.149 (discussing implicit consent and notice associated with the border).

<sup>310.</sup> See Amended Order, supra note 12, at 7 (noting that the GPS installation is a search that "stretches far beyond the conduct of the border to create a 'precise comprehensive record of a person's movements").

<sup>311.</sup> See id. at 6–8 (discussing the installation of the GPS device and subsequent monitoring in the context of *Flores-Montano*, *Jones*, and *Carpenter*).

<sup>312.</sup> United States v. Flores-Montano, 541 U.S. 149, 154 n.2, 156 (2004).

<sup>313.</sup> See Amended Order, supra note 12, at 5-6 (highlighting this open question and how the Ninth Circuit has chosen to handle the question but not utilize it).

<sup>314.</sup> See id. at 5 (determining that it was the "unceasing search that precludes

The analysis thus moves to whether a GPS device should fall under the routine and non-routine search instead.

## a. Routine Searches

If courts analyze the installation of a GPS tracking device under both the routine and non-routine search distinction using the *Jones* distinction, then the Border Search Doctrine should not apply.<sup>315</sup> Unlike a routine search, the attachment of a GPS tracking device is not like a pat-down or the removal of outer garments.<sup>316</sup> Each of the aforementioned limits the degree of intrusiveness to the individual in question.<sup>317</sup> The individual receives notice of the search, can identify the searched item, and understands the full scope of the routine search prior to the intrusion.<sup>318</sup> A GPS tracking device, in contrast, intrudes on an individual's privacy without consent, neglects to provide notice, and reveals more about an individual than a simple routine search.<sup>319</sup>

application of the extended border search doctrine"); see also GPS & Video Installation General concepts and installation techniques, FLEETISTICS, https://www.fleetistics.com/resources/training/gps-installations/ (last visited Feb. 17, 2020) (discussing various GPS installation concepts and providing tutorials for installation) [perma.cc/VKU5-4UPR].

- 315. See United States v. Ramsey, 431 U.S. 606, 618–19 (1977) (discussing routine searches); see also United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993) (highlighting the lower degree of privacy invasion from routine searches); see also United States v. Sandler, 644 F.2d 1163, 1169 (5th Cir. 1981) (noting that pat-down and frisks are routine searches); see also United States v. Jones, 565 U.S. 400, 408 (2012) (concluding that the intrusion on property constituted a search).
- 316. See supra notes 125–128 and accompanying text (commenting on the nature of "routine searches"); see also Amended Order, supra note 12, at 7–8 (discussing the intrusiveness of GPS tracking and how it fits into the Border Search Doctrine and Fourth Amendment jurisprudence).
  - 317. See supra notes 125-128 and accompanying text.
  - 318. See supra notes 125–128 and accompanying text.
- 319. See Jones, 565 U.S. at 404–05, 411–12 (describing the problematic nature of GPS monitoring); see also id. at 430 (Alito, J., concurring) (discussing how "the use of longer term GPS monitoring in investigations... impinges on expectations of privacy"); see also Amended Order, supra note 12, at 7 (noting that "[s]urreptitious surveillance of an individual's movements through placement of a GPS device on a vehicle implicates far greater privacy concerns than the physical integrity of the vehicle").

While an individual can reasonably expect to undergo a routine search upon returning to the border, individuals do not have a reasonable expectation of governmental intrusion to their privacy interests through the installation of a GPS tracking device at the border.<sup>320</sup> The intrusion differs between the two because a routine search is a direct examination of the items or individual at the border in question. 321 In contrast, 322 using a GPS device reveals no information about the individual at the border and merely intrudes on the privacy interests of an individual after crossing.<sup>323</sup> While routine searches do not require a reasonable suspicion prior to inspection, the installation of a GPS tracking device at the border should not fall under a routine search because the intrusion lies in the information gathered away from the border.<sup>324</sup> Because of the heightened degree of intrusiveness and the lack of an actual search at the border, the Border Search Doctrine should not apply to the installation of a GPS tracking device under a routine search.325

#### b. Non-Routine Searches

While a GPS tracking device goes beyond a limited intrusion on an individual, by intruding on the privacy interests of an individual's vehicle and movements, it remains distinguishable

<sup>320.</sup> See PS Rosenzweig, Functional Equivalent, supra note 122, at 1133 (explaining how notice is provided at a recognized border and individuals thus have a lower expectation of privacy); Santana, Almeida-Sanchez, supra note 123, at 238 (highlighting the implicit consent individuals provide to law enforcement at the border); Border Searches and the Fourth Amendment, supra note 146, at 1012

<sup>321.</sup> See Kim, Protecting the U.S. Perimeter, supra note 28 (differentiating routine from non-routine searches, where non-routine includes "strip searches," "prolonged detentions," and others).

<sup>322.</sup> See United States v. Jones, 565 U.S. 400, 404–11 (2012) (concluding that the installation of a GPS violates property interests).

<sup>323.</sup> See United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993) (mentioning that non-routine searches require reasonable suspicion while routine do not); see also Amended Order, supra note 12, at 7 (deciding the "placement of a GPS device at the border necessarily implicates a search away from the border, once the target has gained entry into the country").

<sup>324.</sup> See Amended Order, supra note 12, at 7 (holding the surreptitious surveillance away from the border to result in the border exception not applying).

<sup>325.</sup> See supra notes 315–324 and accompanying text.

from a non-routine search.<sup>326</sup> A non-routine search primarily focuses on the individual in the context of a strip search, body cavity search, or some x-ray searches.327 The disclosure of information or contraband is a result of an intrusion on an individual's personal well-being and space at the border based on reasonable suspicion. 328 The installation of a GPS tracking device, in contrast, focuses on the disclosure of information obtained away from the border and is more intrusive. 329 While the information gathered pertains to the individual driving the vehicle, the information is not readily disclosed at the border and needs to be accumulated.330 The information gathered from a non-routine searched is limited to a person and a specific moment in time.<sup>331</sup> Whereas the information from the GPS tracking device extends to a person's habits and locational privacy as a whole.<sup>332</sup> Consequently, the installation of a GPS tracking device defies both categories of searches.333

Similar to the court's reasoning in *Ignjatov*, "[A]n analysis dependent on the physical aspects of the search [is not] appropriate here where the search extends beyond the installation of the GPS device [at the border]."<sup>334</sup> As such, the Border Search Doctrine should not be applied to the installation and subsequent monitoring of a GPS tracking device at the border.

<sup>326.</sup> See Jones, 565 U.S. at 416 (Sotomayor, J., concurring) (discussing how surveillance techniques evade ordinary checks that constrain law enforcement and chills expressive freedoms).

<sup>327.</sup> See Kim, Protecting the U.S. Perimeter, supra note 28 (describing non-routine searches to include strip searches, body cavity searches, and some x-ray searches).

<sup>328.</sup> See id. (noting how non-routine searches require reasonable suspicion at the time of crossing the border).

<sup>329.</sup> See Amended Order, supra note 12, at 7 (stating that the GPS conducts a search that "stresses far beyond the conduct of the border").

<sup>330.</sup> See id. (mentioning that the information obtained from the border provides a "precise comprehensive record of a person's public movements"); see also United States v. Jones, 565 U.S. 400, 430 (Alito, J., concurring) (describing how long term GPS usage is not a societal expectation).

<sup>331.</sup> See Kim, Protecting the U.S. Perimeter, supra note 28 (discussing non-routine searches to include strip searches, body cavity searches, and some x-ray searches).

<sup>332.</sup> See supra note 329 and accompanying text.

<sup>333.</sup> See supra notes 326–332 and accompanying text.

<sup>334.</sup> Amended Order, supra note 12, at 6.

#### c. Extended Border Search and the Fourth Amendment

As the individual in a vehicle moves away from the border after the installation of the GPS device, the Extended Border Search, albeit hazier in application, should not apply.<sup>335</sup>

While the initial placement of the GPS tracking device occurs at the border, the subsequent monitoring is invasive regardless of the duration.<sup>336</sup> Unlike *Jones*, where the installation of the GPS and its use to obtain information are treated as a singular act that constitutes a search, 337 this continuous monitoring is an extended search.<sup>338</sup> While *Jones* did not delineate whether tracking alone constituted a search, Carpenter bridges this gap. 339 Because tracking can provide the "Government near perfect surveillance," which goes against an "individual's reasonable expectation of privacy as to their whole physical movements," subsequent tracking, though limited to CSLI, violates the Fourth Amendment.<sup>340</sup> "[T]he use of longer term GPS monitoring in investigations . . . impinges on expectations of privacy"341 because it "evades the ordinary checks that constrain abusive law enforcement practices."342 A GPS device allows government agents to track and monitor an individual's location information for an extended period of time. 343 Although the extended border cases

<sup>335.</sup> See infra text accompanying notes 336–352.

<sup>336.</sup> See Amended Order, supra note 12, at 8 (discussing the surreptitious surveillance after installation).

<sup>337.</sup> United States v. Jones, 565 U.S. 400, 404-05, 411-12 (2012).

<sup>338.</sup> See Amended Order, supra note 12, at 8 (noting that even though "the initial placement of the GPS device[] . . . occurred at the border, the subsequent monitoring of data . . . constitutes a continuous search").

<sup>339.</sup> See Carpenter v. United States, 138 S. Ct. 2206, 2210, 2217 (2018) (concluding that seven days of surveillance data to be a search and GPS data to be quite similar to the CSLI obtained).

<sup>340.</sup> See id. at 2217–19 (identifying the similarities between CSLI and GPS even though the Court limited the holding to matters before the Court).

<sup>341.</sup> Jones, 565 U.S. at 430 (Alito, J., concurring).

<sup>342.</sup> Id. at 416 (Sotomayor, J., concurring).

<sup>343.</sup> *Id.* at 430 (Alito, J., concurring) (discussing the duration of tracking); *see* Amended Order, *supra* note 12, at 2–3, 8 (mentioning the installed program's tracking capabilities). While it can be argued that the police merely checked the individual's location infrequently, this fails to recognize that the locational information recorded pertains to an individual's complete movements during a specific period of time. Amended Order, *supra* note 12, at 2–3, 8.

typically involve the physical surveillance of a vehicle after crossing the border, the reasonableness lies in the fact that the subsequent monitoring is in an effort to seize contraband from within the vehicle itself.344 This clashes in the GPS tracking device framework because the installation and subsequent monitoring are not limited to obtaining tangible information regarding the vehicle or items therein, near or at the border, but rather some intangible misconduct away from the border and outside of the vehicle setting.<sup>345</sup> This differs from a gas tank disassembly or an individual x-ray because taking apart a gas tank or taking an x-ray of an individual focus on tangible items present within the object or on the individual at the time of the border crossing. 346 The attachment of a GPS tracking device constitutes a search that exceeds the time of border crossing because it looks to search an intangible element of an individual, either his future location or the entirety of his or her future movements, for an extended period of time.<sup>347</sup> This is especially the case when the tracking program permits the government agents to not only view the locational information for a specific moment but to also download all historic location information from the devices installed.<sup>348</sup> This type of monitoring impinges on an individual's expectation of privacy and may "chill associational and expressive freedoms." 349 "Such tracking is poles apart from the discrete searches conducted under the extended border search doctrine,"350 and thus should not be classified as an extended border search.351

<sup>344.</sup> See United States v. Flores-Montano, 541 U.S. 149, 149 (2004) (discussing this grant of authority to border agents by Congress as a duty to "prevent the introduction of contraband into this country").

<sup>345.</sup> See Amended Order, supra note 12, at 8 (mentioning how law enforcement can download the historic location data which is "poles apart from discrete searches conducted under the extended border doctrine").

<sup>346.</sup> See supra notes 126–127 and accompanying text.

<sup>347.</sup> See Amended Order, supra note 12, at 2–3, 7–8 (analyzing the GPS installation under the Border Search and Extended Border Search Doctrine and concluding that the defendants' motion to suppress should be granted).

<sup>348.</sup> See id. at 2–5, 8 (providing details for the program, Covert Tracker).

<sup>349.</sup> United States v. Jones, 565 U.S.  $400,\ 413{-}18$  (2012) (Sotomayor, J., concurring).

<sup>350.</sup> Amended Order, supra note 12, at 8.

<sup>351.</sup> *Id.* If the attachment of the GPS tracking device is for finding contraband, this still constitutes a search because the installation is a trespass on an individual's property. United States v. Jones, 565 U.S. 400, 404–05 (2012).

Furthermore, travelers do not have notice of a search of this nature.<sup>352</sup> While specific checkpoints of entry can in theory put travelers on notice that searches are likely to be made, this expectation diminishes at "distant border equivalents [that] have no international status."<sup>353</sup> While the initial search occurs at the border and continues on a public roadway, a traveler "has regained an expectation of privacy" once he or she clears the border.<sup>354</sup> An individual typically regains possession of his vehicle after the installation of a GPS tracking device because law enforcement officers want to monitor the individual away from the border.<sup>355</sup> The surreptitious installation of the GPS tracker thus constitutes a physical trespass without notice or consent and cannot be classified as an extended border search.<sup>356</sup> Physical surveillance contrasts from GPS monitoring because no intrusion into the physical domain of an individual occurs in the former,<sup>357</sup> while the

Even if the contraband is in the vehicle near the border, courts have found that distance to the border is not enough in itself to validate a search and requires reasonable suspicion. United States v. Rangel-Partillo, 586 F.3d 376, 376 (5th Cir. 2009). If the contraband is not located at the border at the time of crossing, then it similarly should not fall under the Border Search Doctrine, for distance to the border alone is not enough. *Id.* If agents are unable to determine whether or not the Border Search Doctrine applies, when dealing with the possible presence of contraband, then as Justice Alito posited in *Jones*, "police may always seek a warrant" if uncertain "whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment Search. *Jones*, 565 U.S. at 430–31 (Alito, J., concurring).

- 352. See PS Rosenzweig, Functional Equivalent, supra note 122, at 1133 (discussing how travelers are implicitly put on notice because of the presence of a border); see also Santana, Almeida-Sanchez, supra note 123, at 238 (discussing how an individual's lowered expectation of privacy at the border increases as they get farther from the border).
  - 353. PS Rosenzweig, Functional Equivalent, supra note 122, at 1133.
- 354. United States v. Cotterman, 709 F.3d 952, 961–62 (9th Cir.) (en banc), cert. denied, 571 U.S. 1156 (2014) (delineating between an individual regaining his expectation of privacy versus Cotterman, who never regained his laptop because it did not clear the border).
- 355. See Amended Order, supra note 12, at 2–5, 8 (discussing the information gained after installation).
- 356. See id. at 2–5, 7–8 (concluding that prolonged surveillance could not be classified as either a border search or an extended border search).
- 357. See id. at 7 (describing how "[w]hile the placement of a GPS device on a vehicle falls short of an intrusion 'akin to reading a diary line by line' . . . data collection inherent in GPS monitoring exceeds suspicionless searches authorized in the border vehicle cases"); see also Santana, Almeida-Sanchez, supra note 123, at 238 (discussing implicit consent in border search cases).

government in the latter scenario "trespassorily insert[s] the information-gathering device" to the privacy property of an individual.<sup>358</sup> Travelers, for this reason, do not have notice that they may be subjected to a search of this nature.

## d. GPS Devices and Current Policies

This Note discussed two border policies known to date.<sup>359</sup> If courts analyze the existing border policies in conjunction with the installation of a GPS tracking device, the Border Search Doctrine should not apply. The CBP Border policy distinguishes electronic searches at the border to be either "basic" or "advanced" and assigns a level of suspicion dependent on the type of search labeled by the government.<sup>360</sup> The DHS GPS Policy appears to mold a framework between existing Fourth Amendment jurisprudence and the Border Search Doctrine.<sup>361</sup>

The CBP Border policy is meant for electronic devices acquired at the border upon entry or departure.<sup>362</sup> It however is not applicable to the vehicle context.<sup>363</sup> This is because the installation of the GPS device and subsequent monitoring is not a stationary search at the border like an electronic device.<sup>364</sup> While the GPS device could be considered external equipment used by border agents to "review, copy, and/or analyze [the vehicle's] contents,"<sup>365</sup>

<sup>358.</sup> United States v. Jones, 565 U.S. 400, 408-11 (2012).

<sup>359.</sup> See U.S. Customs and Border Protection 2018, supra note 189 (outlining the current policy for electronic devices); see also Allen Declaration, supra note 17, at 1–3 (describing the policy and authority behind the 48-hour policy law enforcement utilized to justify the installation in *Ignjatov*).

<sup>360.</sup> See U.S. Customs and Border Protection 2018, supra note 189 (categorizing the search and outlining the differences).

<sup>361.</sup> See Allen Declaration, supra note 17, at 1–3 (describing the policy's authority).

<sup>362.</sup> See U.S. Customs and Border Protection 2018, supra note 189 (listing the subject of the guideline to be "border search of electronic devices").

<sup>363.</sup> See id. (naming the purpose to be providing guidance "in computers, tablets, removable disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches").

<sup>364.</sup> See Amended Order, supra note 12, at 7 (concluding the search extended beyond the border).

<sup>365.</sup> See U.S. Customs and Border Protection 2018, supra note 189 (covering

the analysis is not complete at the border and the individual is not notified of the advanced search.<sup>366</sup> Moreover, the vehicle is merely a conduit for the physical movements of an individual rather than the actual item examined.<sup>367</sup> This does not mean that the vehicle itself or the individual should not be subject to a search at the border.<sup>368</sup> Instead, because the information sought from the installation of a GPS device does not pertain to the vehicle but rather the individual's movements and possible unconfirmed misconduct away from the border, this border policy should not apply to GPS tracking devices.<sup>369</sup>

The DHS GPS Policy from *Ignjatov* is more difficult to explain, given the lack of information in the factual record.<sup>370</sup> However, based on the facts known, a court would not find the border policy to be valid under the Border Search Doctrine or Fourth Amendment jurisprudence. HSI bases its border policy on the belief that it successfully merges the Supreme Court's decisions in *Jones* and *Flores-Montano* with the Border Search Doctrine.<sup>371</sup> Nevertheless, a clear disparity exists between the three.

The first divergence is the fact that the Border Search Doctrine and *Flores-Montano* focus on searches of an individual and vehicles at the border.<sup>372</sup> While the extended border doctrine examines a secondary search away from the border, that search is clearly delineated and focused on a particular item, like electronic devices or a vehicle.<sup>373</sup> *Jones* treats the GPS installation and

the scope of the search of an electronic device).

<sup>366.</sup> See Amended Order, supra note 12, at 7 (discussing how "the concerns animating the border search doctrine, namely the integrity of the border, diminish, and the robust Fourth Amendment requirements adhere" once the search extends beyond the border continuously in duration).

<sup>367.</sup> *See id.* at 2–3, 7–8 (highlighting the tracking program and its ability to trace the individual for a set interval, which law enforcement agents determined).

<sup>368.</sup> See id. at 7–8 (describing how it is the extensive and intrusive nature of the search that makes a GPS tracking device problematic).

<sup>369.</sup> See U.S. Customs and Border Protection 2018, supra note 189 (providing a list of items it governs and vehicles are not one of them).

<sup>370.</sup> See Allen Declaration, supra note 17, at 1–3 (discussing the only facts known about the 48-hour policy).

<sup>371.</sup> See id. at 1-3 (listing the authorities the 48-hour policy is based on).

<sup>372.</sup> See United States v. Flores-Montano, 541 U.S. 149, 149 (2004) (discussing a vehicle search at the border); see supra notes 116–139 and accompanying text.

<sup>373.</sup> See supra notes 140-170 and accompanying text.

subsequent use to track a vehicle as a singular act.<sup>374</sup> While *Jones* did not determine whether tracking alone constituted a search, *Carpenter* determined that acquiring location information for seven days violates the Fourth Amendment because "individuals have a reasonable expectation of privacy in the whole of their physical movements."<sup>375</sup> Tying the two concepts together, the Supreme Court in *Carpenter* appears to extend *Jones* to include tracking as a search under the Fourth Amendment.<sup>376</sup>

As such, the installation of the GPS device and subsequent monitoring do not fit clearly within the Border Search Doctrine or Flores-Montano.377 This is because the installation of a GPS tracking device and its subsequent surveillance are a continuous search away from the border.<sup>378</sup> The search is not stationary like that of a traditional border search or the vehicle search in Flores-Montano.<sup>379</sup> The device, instead, not only offers real-time locational data, but it also records and stores these data for others to examine at a later time. 380 Because officials can alter the amount of data acquired from the device, the GPS tracking device is an extension of a traditional search and occurs outside of the border region.<sup>381</sup> Following *Carpenter*, because individuals have an expectation of privacy in the whole of their movements, 382 this is a search under continuous monitoring the

<sup>374.</sup> United States v. Jones, 565 U.S. 400, 404–05, 411–12 (2012) (holding "that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search'").

<sup>375.</sup> Carpenter v. United States 138 S. Ct. 2206, 2213–20 (2018).

<sup>376.</sup> See Jones, 565 U.S. at 404–05, 411–12 (discussing the intrusion to property from the installation); see also Carpenter, 138 S. Ct. at 2213–20 (describing how surveillance is a search because individual's have a reasonable expectation of privacy in the whole of their movements).

<sup>377.</sup> See supra notes 371–376 and accompanying text.

<sup>378.</sup> See Amended Order, supra note 12, at 7–8 (discussing the problematic nature of the GPS installation and subsequent monitoring).

<sup>379.</sup> See id. at 7–8, 15 (mentioning Flores-Montano and unwilling to find GPS installation and subsequent monitoring to be on the same foot).

<sup>380.</sup> See Amended Order, supra note 12, at 2-3 (discussing the program's tracking capabilities).

 $<sup>381.\</sup> See\ id.$  at 2–3, 7–8 (mentioning the changes in tracking intervals and continuous search).

<sup>382.</sup> Carpenter, 138 S. Ct. at 2213–20 (holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI").

Amendment.<sup>383</sup> This falls outside of the Border Search Doctrine, the extended border search, and *Flores-Montano*'s sphere of influence.<sup>384</sup>

Jones does not rectify this conundrum because the Court focused on the installation and its use which intruded on the individual's property and privacy. Jones did not focus on the vehicle alone or the fact that the individual was driving on public roadways. Instead, the Court zeroed in on the intrusion caused by the installation of the device. The intrusion into the private property of an individual and his or her movements became the ultimate problem. See As such, analyzing the installation of a GPS device and its subsequent tracking solely under a vehicle search context under the Border Search Doctrine or Flores-Montano is an insufficient justification for the border policy.

Furthermore, based on the three authorities presented, it is unclear as to which doctrine governs once an individual clears the border. <sup>390</sup> Utilizing only the three authorities presented, if *Jones* takes over immediately after clearing the border, then the installation of the device is a search under the Fourth Amendment. <sup>391</sup> This is because the majority in *Jones* focused on the intrusion to the individual rather than ongoing tracking. <sup>392</sup> Therefore, the installation itself, which is a trespass on an individual's property, controls <sup>393</sup> and lacks support as a border policy by Fourth Amendment jurisprudence.

<sup>383.</sup> See Amended Order, supra note 12, at 7–8 (refusing to allow continuous tracking to fall under the border search exception).

<sup>384.</sup> See supra notes 372–383 and accompanying text.

 $<sup>385.\</sup> See$  United States v. Jones, 565 U.S.  $404,\ 404-05,\ 411-12$  (2012) (applying the common-law of trespass).

<sup>386.</sup> *Id*.

<sup>387.</sup> *Id*.

<sup>388.</sup> See id. at 404–05, 408–12 (describing the physical intrusion to property).

<sup>389.</sup> See supra notes 372–388 and accompanying text.

<sup>390.</sup> See Allen Declaration, supra note 17, at 1–3 (discussing the only known facts of the policy).

<sup>391.</sup> See Jones, 565 U.S. at 400, 410–11 (determining the GPS installation to be a search because it trespassed into the individual's property).

<sup>392.</sup> *Id.* at 409-12 (noting that by physically attaching a device to Jones' Jeep, "officers encroached on a protected area").

 $<sup>393.\</sup> Id.$  at  $404-05,\ 411-12$  (noting that intrusion in the form of the government physically occupying private property would have been considered a

The Border Search Doctrine and *Flores-Montano* should not apply to the GPS installation once an individual clears the border.<sup>394</sup> *Flores-Montano* concerns a stationary search of a vehicle at the border,<sup>395</sup> while the Border Search Doctrine concerns searching an individual, vehicle, or item at or near the border.<sup>396</sup> Whereas, the installation of a GPS device obtains information outside of the vehicle context for misconduct away from the border.<sup>397</sup>

If the policy allows for authorities outside of the three listed, then *Carpenter* should apply.<sup>398</sup> *Carpenter* focused on the tracking itself and determined that "individuals [have a] reasonable expectation of privacy as to their whole physical movements."<sup>399</sup> Because the tracking showcased an "exhaustive chronicle of location information," the Court determined that seven days of historical CSLI data constituted a search.<sup>400</sup> Accordingly, even if an individual clears the border and reacquires a heightened expectation of privacy while traversing on a public roadway, the subsequent tracking, regardless of the installation, is a search because of the intrusion on an individual's movements.<sup>401</sup> Based on this line of reasoning, regardless of the authorities used, the border policy is a search under the Fourth Amendment based on the reasoning in *Jones* and *Carpenter*.<sup>402</sup>

While the border policy states that it allows for "limit[ed] warrantless GPS monitoring to 48 hours, with the exception of airplanes, commercial vehicles, and semi-tractor

<sup>&#</sup>x27;search' within the meaning of the Fourth Amendment when it was adopted").

<sup>394.</sup> See discussion supra Section II.B.

<sup>395.</sup> See United States v. Flores-Montano, 541 U.S. 149, 149 (2004) (outlining the facts to the case).

<sup>396.</sup> See discussion supra Section II.B.

<sup>397.</sup> See Amended Order, supra note 12, at 7 (discussing the information acquired and search).

<sup>398.</sup> See discussion supra Section II.B.

<sup>399.</sup> Carpenter v. United States, 138 S. Ct. 2206, 2210, 2217 (2018).

<sup>400.</sup> Id. at 2219-20.

<sup>401.</sup> See id. at 2210, 2217, 2219–20 (discussing the ramifications of surveillance of this nature and how it goes against an individual's reasonable expectation of privacy in the whole of their movements); see also United States v. Jones, 565 U.S. 400, 411–12 (2012) (disregarding the fact that the vehicle traversed on public roadways).

<sup>402.</sup> See supra notes 399-401 and accompanying text.

trailers... [because they] have a significantly reduced expectation of privacy in the location of their vehicles,"<sup>403</sup> existing precedent and literature do not substantiate this claim. While *Knotts* and *Karo* establish a diminished expectation of privacy on public roadways, they did not explicitly distinguish specific privacy interests based on the vehicles on the road or apply their reasoning to the border.<sup>404</sup> Similarly, *Jones* did not establish a reduced expectation of privacy based on the vehicle driven.<sup>405</sup> Instead, *Jones* focused on the intrusion to privacy interests and property.<sup>406</sup> It is thus unclear why those particular vehicles have a reduced expectation of privacy in their locations.<sup>407</sup>

While *Jones* did not explicitly pinpoint a timeframe of constant surveillance to constitute a search, both concurrences took a firmer stance, which *Carpenter* endorsed, 408 for *Carpenter* concluded that seven days of historical CSLI data represented a search. 409

While *Carpenter* was a narrow ruling focusing only on the matters before the Court, the logic behind the ruling stands.<sup>410</sup> Surveillance data offers "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual

<sup>403.</sup> Allen Declaration, supra note 17, at 1–3.

<sup>404.</sup> See United States v. Knotts, 460 U.S. 276, 276, 286 (1983) (finding no violation from the tracking and surveillance); see also United States v. Karo, 468 U.S. 705, 706 (1984) (concluding no violation under the *Katz* test, even though container contained a beeper).

<sup>405.</sup> See Jones, 565 U.S. at 401, 404–05, 408–12 (determining that the trespass on the vehicle is why the installation of a GPS device violates the Fourth Amendment).

<sup>406.</sup> See id. at 408–12 (utilizing common-law trespass rather than Katz to find the installation to be a search).

<sup>407.</sup> See supra notes 403–406 and accompanying text.

<sup>408.</sup> See Jones, 565 U.S. at 413–19 (Sotomayor, J., concurring) (determining that surveillance of this nature "chills associational and expressive freedoms"); see also Jones, 565 U.S. at 419–31 (Alito, J., concurring) (describing that long-term GPS surveillance is a search, like the four weeks utilized in Jones); see also Carpenter, 138 S. Ct. at 2206–08 (recognizing individuals have a reasonable expectation in the whole of their movements).

<sup>409.</sup> Carpenter v. United States, 138 S. Ct. 2206, 2210, 2214–19 (2018) (holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI").

<sup>410.</sup> See id. at 2217–19 (describing how the holding did not extend past the matter before the Court).

associations."411 Monitoring is "remarkably easy, cheap, and efficient compared to traditional tools . . . [and] [w]ith just the click of a button, the Government can access...[a] repository of historical location information at practically no expense."412 This type of "retrospective quality of data [] gives police access to a category of information otherwise unknowable," and gathered without consent.413 Forty-eight hours may seem like a brief duration, but dependent on the speed, an individual could travel a distance of over 3000 miles. 414 This is almost thirty times the reasonable distance defined by statutory authority. 415 This is an expansive period of time for law enforcement to gather continuous "near perfect surveillance" 416 and impinges on an individual's expectation of privacy. 417 To put it into perspective, it takes thirty-nine hours to travel from California to Virginia, which are 2,646 miles apart.418 A disconnect thus exists between the level of authority defined by federal statute and DHS GPS Policy. An individual's movements during this time frame of forty-eight hours would provide an intimate look into an individual's life, and "[s]uch a chronicle implicates privacy concerns far beyond those considered" in Carpenter. 419 The forty-eight-hour exception

<sup>411.</sup> Id. at 2217; Jones, 565 U.S. at 415 (Sotomayor, J., concurring).

<sup>412.</sup> Carpenter, 138 S. Ct. at 2217-18.

<sup>413.</sup> Id. at 2218.

<sup>414.</sup> See Unit 18 Section 2: Calculating speed, distance and time, CENTRE FOR INNOVATION IN MATHEMATICS TEACHING, https://www.cimt.org.uk/projects/mepres/book8/bk8i18/bk8\_18i2.htm (last visited Feb. 14, 2020) (calculating distance by multiplying the amount of time with the speed and if an individual is going 65mph for 48 hours, they can traverse over 3000 miles) [perma.cc/SSV8-KBJV].

<sup>415.</sup> See 8 C.F.R. § 287.1(b) (2018) (defining "reasonable distance").

<sup>416.</sup> See Carpenter, 138 S. Ct. at 2210, 2217-19 (recognizing the privacy interests of individuals against intrusive law enforcement techniques).

<sup>417.</sup> See United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (commenting on why long-term surveillance is more detrimental than short-term surveillance).

<sup>418.</sup> Driving Directions from California to Virginia, GOOGLE MAPS, http://maps.google.com (last visited Sept. 20, 2020) (follow "Directions" hyperlink; then searching starting point field for "California" and search destination field for "Virginia") [perma.cc/6KEP-LZ72].

<sup>419.</sup> See Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018) (discussing why surveillance of this nature is problematic).

summarized in the border policy is thus a search under the Fourth Amendment, even with the limited facts known at this time. 420

Limitations accordingly exist to the Border Search Doctrine, regardless of the controversial policies in existence. <sup>421</sup> As dictated by the court in *Ignjatov*, "Once the entity at issue is beyond the border, the concerns animating the border search doctrine, namely the integrity of the border, diminish, and the robust Fourth Amendment requirements adhere." <sup>422</sup> It thus follows, based on *Jones* and *Carpenter*, that the installation of a GPS tracking device is a search under the Fourth Amendment that is not subject to the border search exception. <sup>423</sup>

## V. Transparency and Accountability: Why Courts Matter

While a great deal of overlap exists between the Fourth Amendment and the Border Search Doctrine, one must ultimately yield, as seen in *Ignjatov* and described above. 424 However, an impediment remains: A lack of transparency persists for policies along the border. While the EFF and DHS continue their ongoing litigation, privacy interests are at an impasse. 425 This is problematic because obscure policies diminish an individual's trust in the governing system, which weakens governmental authority thereby diminishing the foundation of a legitimate democratic government. 426 While *Jones* and *Alasaad* serve as a barrier of sorts

<sup>420.</sup> See Gruel Declaration, supra note 10, at 1–4 (explaining during sixteen years as an AUSA and ten years as Chief of the General Crimes Section, neither he nor anyone asked had heard of "a border exception permitting . . . warrantless installation of . . . GPS tracking device[s] or some sort of 48 hour-rule," or "this '48 hour rule' or the 'commercial vehicle exception").

<sup>421.</sup> See discussion supra Section II.B.

<sup>422.</sup> Amended Order, supra note 12, at 7.

<sup>423.</sup> See discussion supra Sections III.A–B, IV.A–B.

<sup>424.</sup> See discussion supra Sections III.A–B.

<sup>425.</sup> See EFF Order, supra note 22 (laying out a schedule through February 11, 2021).

<sup>426.</sup> See Eric E. Citron, Right and Responsibility in Fourth Amendment Jurisprudence: The Problem with Pretext, 116 YALE L. J. 1072, 1104–106 (2007) (arguing that a relationship between citizenry and the "power of the state and its police force" is "one of trust" for "a fiduciary duty [] runs from the police to the citizenry that granted them their unique powers in the first place").

for privacy interests,<sup>427</sup> policy transparency in congruence with established precedent is necessary to ensure the privacy rights of both citizens and noncitizens alike.

An individual has "full protection in person and in property," which is "a principle as old as the common law." 428 Political, social, and economic changes, however, result in the "recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."429 On a foundational level, individuals have a baseline regarding privacy. 430 This includes a "right to be left alone."431 The Fourth Amendment developed "upon the idea that integral to the Constitution and our societal view of government is a reciprocal trust between the government and its citizens."432 "This mandate from the citizenry legitimatizes government action; however, only if the citizenry's decision itself is an informed and free choice such that the government can claim that it has true consent of the governed."433 Achievement of this mandate can only be done if the government "does not imperil the citizenry's ability to give its consent in an informed and free manner."434 However, the advancements of technology fragment these expectations and

<sup>427.</sup> See United States v. Jones, 565 U.S. 400, 400 (2012) (holding that the installation of a GPS device violates the Fourth Amendment); see also Alasaad Order, supra note 202 (determining that reasonable suspicion is required for both a basic and advanced search at the border for electronic devices).

<sup>428.</sup> See Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARVARD L. REV. 193, 193 (1890) [hereinafter Warren & Brandeis, Right to Privacy] (protesting against the intrusive activities of the journalists in those days and suggesting individuals maintain privacy even against those activities).

<sup>429.</sup> Id.

<sup>430.</sup> *Id.* at 198 (stating that "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others").

<sup>431.</sup> *Id.* at 193–94; *see also* Goldman v. United States, 316 U.S. 129, 136–37 (1942) (Murphy, J., dissenting) (emphasizing that "the Fourth Amendment puts a restraint on the arm of the government and prevents it from invading the sanctity of a man's home or his private quarters . . . to prevent oppression and abuse of authority").

<sup>432.</sup> Scott E. Sundby, Everyone's Fourth Amendment: Privacy or Mutual Trust between Government and Citizen, 94 Colum. L. Rev. 1751, 1777 (1994) [hereinafter Sundby, Everyone's Fourth]; see also, id. at 1771 (discussing trust as a constitutional value).

<sup>433.</sup> *Id*.

<sup>434.</sup> *Id*.

jeopardize this underlying trust. 435 "The Fourth Amendment as a privacy-focused doctrine has not fared well with the changing time of an increasingly non-private world and a judicial reluctance to expand individual rights."436 "The problem [is that] privacy in new technologies 'is usually complex."437 "Developments such as growing government regulation and expanding technological capacity [] have robbed the 'right to be left alone."438 "The result is a complex and often-fluctuating relationship between surveillance and privacy."439 This is because technological change can result in "preexisting forms of surveillance [becoming] more intrusive" or the opposite effect, which upsets both law enforcement's interpretation and privacy interests. 440

Fourth Amendment precedent currently "frames the issue as a binary choice between the antagonistic interests—the government's law enforcement needs and the individual's privacy interest." "Rights [however] are not simply enclaves of protection from government interference but also affect the citizen's view of his or her role in society." To put it in simpler terms, rights help frame an individual's reasonable expectation of his or her own privacy interests, and in the Fourth Amendment context, this can heavily influence whether a government intrusion constitutes a search. It is therefore important to understand both the technological innovation and the ultimate policies established in

<sup>435.</sup> See Orin S. Kerr, The Fourth Amendment and New Technologies, 102 MICH. L. REV. 801, 859 (2004) [hereinafter Kerr, The Fourth Amendment] (discussing ramification of new technology).

<sup>436.</sup> Sundby, Everyone's Fourth, supra note 432, at 1771.

<sup>437.</sup> Kerr, *The Fourth Amendment*, *supra* note 435, at 877; *see also* Stephen Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. REV. 245, 262 (2002) (noting the complexities of establishing law involving changing technologies and public perceptions, while "balancing [the] value in light of predictions about the technological future").

<sup>438.</sup> Sundby, *Everyone's Fourth*, *supra* note 432, at 1777 (noting the decline of privacy rights when there is a lack of accountability).

<sup>439.</sup> Kerr, The Fourth Amendment, supra note 435, at 859.

<sup>440.</sup> Id. at 865.

<sup>441.</sup> See Sundby, Everyone's Fourth, supra note 432, at 1784 (highlighting a deficiency in current Fourth Amendment jurisprudence).

<sup>442.</sup> *Id*.

<sup>443.</sup> See discussion supra Sections II.A–B.

conjunction with them to promote trust and accountability between the citizenry and government.<sup>444</sup>

"An implicit linkage between privacy and visibility is deeply embedded in privacy doctrine."445 Some privacy skeptics argue that "information conveyed by most individual items of personal data is too banal to trigger privacy interest."446 Yet, transparency and accountability work hand-in-hand.447 "Transparency alters the parameters of evolving subjectivity [of spaces and places whereas surveillance exposure alters the capacity of places to function as contexts within which identity is developed and performed."448 Technology, however, should not be solely blamed for "this broken link between transparency and public accountability."449 Instead. Professor Shkabatur argues that this discrepancy is due to agencies being able to "retain control over regulatory data and thus withhold information that is essential for public accountability purposes."450 Consequently, "transparency policies—and not only their rhetoric—should focus on accountability related information."451

To do this, Professor Shkabatur proposes requiring "agencies to explain and justify their decisions" outside of the notice and comment period, instead of "letting agencies disclose whatever data they choose." <sup>452</sup> A requirement of this nature is necessary

<sup>444.</sup> See Jennifer Shkabatur, Transparency With(out) Accountability: Open Government in the United States, 31 YALE L. & POLICY REV. 79, 79–80 (2012) [hereinafter Shkabatur, Transparency With(out) Accountability] (evaluating online transparency and agency accountability).

<sup>445.</sup> Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 182 (2008) [hereinafter Cohen, *Privacy*] (discussing how privacy and visibility go hand-in-hand).

<sup>446.</sup> See id. at 183 (describing the evolution of the privacy doctrine).

<sup>447.</sup> See Shkabatur, Transparency With(out) Accountability, supra note 444, at 119 (highlighting why transparency is important with technological advancement).

<sup>448.</sup> See Cohen, Privacy, supra note 445, at 194 (highlighting the complementary effects of exposure and transparency).

<sup>449.</sup> See Shkabatur, Transparency With(out) Accountability, supra note 444, at 81 (outlining the argument for the article).

<sup>450.</sup> Id.

<sup>451.</sup> Id.

<sup>452.</sup> *Id.* at 120; see also Christopher Slobogin, *Policing As Administration*, 165 U. PENN. L. REV. 1, 1 (2016) (advocating for "[p]olice agencies [to] be governed by the same administrative principles that govern other agencies . . . to engage in

because "[a] major pitfall of the current transparency architecture is that it largely allows agencies to decide what types of information should be placed in the public domain."<sup>453</sup> This type of intrusion on "reciprocal trust" "implicates the Fourth Amendment and is jeopardized when the government is allowed to intrude into the citizenry's lives without a finding that the citizenry has forfeited a society's trust to exercise its freedoms responsibly."<sup>454</sup>

GPS tracking at the border fits well into this context. 455 Currently, an individual implicitly consents to a search both upon exiting and returning to the United States. 456 He or she has a reasonable expectation based on the presence of the border and thus acquires notice of an impending search prior to arriving at the border. 457 Individuals consent to this search because of both respect for the sovereign borders of a country and trust that the government will not overstep. 458 Yet, under "classic" Fourth Amendment precedent, individuals have an expectation of privacy for their property, and the installation of a GPS tracking device is a trespass which violates the Fourth Amendment. 459 Combining the two doctrines without more leaves citizens in a bind, for it alters an individual's "right to be left alone" while damaging the reciprocal trust for the government. 460 The opaque policy "alters the parameters of evolving subjectivity," and this shift in balance poses problematic consequences if not rectified. 461

notice-and-comment rulemaking or a similar democratically oriented process and avoid arbitrary and capricious rules").

<sup>453.</sup> Shkabatur, Transparency With(out) Accountability, supra note 444, at 120.

<sup>454.</sup> See Sundby, Everyone's Fourth, supra note 432, at 1777 (discussing government interests against the trust of citizenry).

<sup>455.</sup> See Amended Order, supra note 12, at 1–15 (highlighting the problematic nature of GPS installation at the border).

<sup>456.</sup> See Santana, Almeida-Sanchez, supra note 123, at 238 n.149 (noting how individuals who leave the borders implicitly consent and are put on notice of a search upon their return).

<sup>457.</sup> See id. (discussing the border crossing and certain justifications for it).

<sup>458.</sup> See id. (providing justifications over the years for the border search).

<sup>459.</sup> See United States v. Jones, 565 U.S. at 400, 400 (2012) (holding that the installation of a GPS device is a search under the Fourth Amendment).

<sup>460.</sup> See id. (noting that an individual has an expectation of privacy to his or her property); see also Cohen, Privacy, supra note 445, at 194 (discussing privacy as a concept and what happens to privacy expectations when violated).

<sup>461.</sup> See Cohen, Privacy, supra note 445, at 194 (mentioning that "[t]he

"One of the most frequent objections to transparency . . . is that doing so would allow criminals to more skillfully evade" detection, thus hindering national security interests. 462 "The need for secrecy [however] is not nearly as acute as it may seem."463 First, a secrecy argument against disclosures of regulations regarding deterrence is unnecessary. 464 For the entire deterrence-based techniques, like administrative inspections, "is to use the threat of detection to keep people within the lines of law."465 "[T]here is [accordingly] no plausible rationale for shielding department policies regarding the use of these tactics from public debate."466 A similar argument exists at the border. GPS tracking aims to deter and detect individuals suspected of criminal conduct. 467 Without proper notice and disclosure of GPS policies at the border, 468 an individual lacks the requisite threat of detection to remain in the "lines of the law." 469 Deterrence then becomes moot in this context.<sup>470</sup> However, in regards to more sensitive areas of policing, Friedman and Ponomarenko argue that "the key distinction is between operational details and governing law."471

effects of exposure and transparency are complementary").

<sup>462.</sup> See Barry Friedman & Maria Ponomarenko, Democratic Policing, 90 N.Y.U. L. REV. 1827, 1884 (2015) [hereinafter Friedman & Ponomarenko, Democratic Policing] (outlining when secrecy is permissible).

<sup>463.</sup> Id.

<sup>464.</sup> See id. (discussing secrecy and deterrence-based techniques).

<sup>465.</sup> Id.

<sup>466.</sup> Id.

<sup>467.</sup> See United States v. Flores-Montano, 541 U.S. 149, 149 (2004) (noting how Congress grants executive plenary authority for routine searches at the border to not only regulate border duties but to prevent contraband from entering into this country); see also United States v. Caicedo-Guarnizo, 723 F.2d 1420, 1422 (9th Cir. 1984) (highlighting that the validity of a search depends on the totality of the circumstances and being reasonably certain that contraband was acquired after crossing the border).

<sup>468.</sup> See discussion supra Part III; see also Allen Declaration, supra note 17, at 2–3 (discussing the GPS policy utilized in *Ignjatov* without disclosing the authority behind the policy or when it came into fruition).

<sup>469.</sup> Friedman & Ponomarenko, Democratic Policing, supra note 462, at 1884.

<sup>470.</sup> See id. (stating that "[s]ecrecy makes the least sense as an argument for avoiding regulation when it comes to policing based explicitly on deterrence").

<sup>471.</sup> See id. at 1884–85 (distinguishing between deterrence policies and sensitive policies).

Operational details, such as investigation techniques and department protocols, are types of things that do not need to be revealed because revealing this information encourages circumvention of governmental authority. 472 In contrast, governing law includes the department's rules regarding use of these techniques, including the level of suspicion required, and can be made public without undercutting governmental interests. 473 DHS and CBP's forty-eight-hour border policy falls primarily under the governing law characterization. 474 EFF's FOIA request sought "policies and/or procedures regarding the use of the GPS tracking devices on vehicles crossing the border" and "training manuals and/or training materials."475 While procedures could arguably fall into "operational details," policies and training materials fall more in line with "governing law" because revealing this information merely illustrates the rationale and justification of the agency, which bolsters credibility and encourages greater reciprocal trust in the governing system. 476 Questions remain from the information disclosed in *Igniatov*. Unlike disclosing information regarding the specific "timing of [electronic surveillance technique[s] use[d], and the specific location where they were employed,"477 the disclosure of policies and/or procedures regarding the use of GPS tracking devices on vehicles focuses instead on allowing the public to "make informed decisions about policing policy."478

FOIA exceptions should apply to "operational details" to maintain governmental interests, but in regards to matters of governing law, the emphasis similarly should be on allowing the

<sup>472.</sup> See id. at 1885 (differentiating between operational details and governing law).

<sup>473.</sup> See id. (commenting on how governing rules differ from logistics for undercover operations).

<sup>474.</sup> See Allen Declaration, supra note 17, at 2–3 (providing the only known specifics to date regarding the policy).

<sup>475.</sup> EFF Complaint, *supra* note 1, at 1.

<sup>476.</sup> See Shkabatur, Transparency With(out) Accountability, supra note 444, at 79–80 (describing the benefits of agency transparency on the citizenry).

<sup>477.</sup> See Lewis-Bey v. United States, 595 F. Supp. 2d 120, 137–38 (D.D.C. 2009) (protecting and withholding specific undercover investigative techniques).

<sup>478.</sup> See Friedman & Ponomarenko, Democratic Policing, supra note 462, at 1886–87 (considering how a number of police agencies already make their manuals publicly available).

public "to make informed decisions about policing policy." <sup>479</sup> By allowing a degree of notice and public participation, public discourse increases and shifts "the parameters of evolving subjectivity," thereby reshaping the sphere of transparency. <sup>480</sup>

Ex post reasoning "would require public officials to explain the values and priorities that underlie their decisions,"481 which would "require|| participants to move away from positions too obviously tailored to their self-interest .... "482 Without disclosure, "surveillance [in a free society] can have a substantial chilling effect on thought, reading habits, and private speech."483 This effect can alter the balance in reciprocal trust and leave individuals blindsided. 484 A need for transparency is thus necessary to efficiently protect privacy interests as technology advances, for "[t]rust can add nuance and force to foundational privacy concepts such as confidentiality, transparency and security by reimagining them as discretion, honesty, and protection."485 Policy transparency is thus an integral part in maintaining the trust of the citizenry within the system. 486 The lack of transparency in current GPS border policies will only erode the "balance in reciprocal trust and leave individuals blindsided" as they cross the border. 487 However, policy transparency alone is not enough to

<sup>479.</sup> See Shkabatur, Transparency With(out) Accountability, supra note 444, at 121 (commenting on how FOIA exceptions make implementing disclosure of information outside of a notice and comment period difficult).

 $<sup>480.\ \</sup> See$  Cohen,  $Privacy,\, supra$  note 445, at 194 (stressing the importance of transparency).

<sup>481.</sup> Id. at 122.

<sup>482.</sup> *Id.* at 121.

<sup>483.</sup> Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 431–32, 456 (2016) [hereinafter Richards, *Taking Trust Seriously*] (examining the consequences of disregarding trust in privacy law).

<sup>484.</sup> See Cohen, Privacy, supra note 445, at 194 (highlighting the effects of exposure and transparency).

<sup>485.</sup> See Richards, Taking Trust Seriously, supra note 483, at 457 (focusing on the detrimental effects of a lack of transparency).

<sup>486.</sup> See id. (stating that "trust can rejuvenate privacy law and policy").

<sup>487.</sup> See discussion supra Sections III.A–B.

protect privacy interests.<sup>488</sup> Technological changes to the privacy status quo also require flexible and adaptable rules in response.<sup>489</sup>

While the development of Fourth Amendment jurisprudence may seem drawn-out and sluggish in response to technological change, there are a number of benefits to relying on Fourth Amendment precedent rather than waiting on legislation.<sup>490</sup> "When the Fourth Amendment covers a particular law enforcement activity, it provides a set of rules to regulate it."<sup>491</sup> A degree of flexibility exists in Fourth Amendment rules, which balances "privacy interests and law enforcement needs."<sup>492</sup> Furthermore, the Court has made exceptions to the warrant and probable cause requirements to "accommodate a wide range of government investigative activity within the protective framework of the Fourth Amendment."<sup>493</sup>

Professor Kerr argues that "[j]udicial rulemaking is limited by strong stare decisis norms that limit the ability of judicial rules to change quickly; in contrast, legislatures enjoy wide-ranging discretion to enact new rules." While Professor Kerr's argument holds merit to a degree, due to the slow nature of Congressional decision-making, "[t]he answer to the problem of creating rules to regulate law enforcement and new technologies is not to call for judicial caution and leave it to legislatures to draft the primary law. Rather, the answer is simply to craft better rules." Courts need to be better informed regarding the technology in play, but to do so requires a degree of transparency by agencies.

<sup>488.</sup> See discussion supra Section II.A.

<sup>489.</sup> See discussion supra Section II.A.

<sup>490.</sup> Daniel J. Solove, Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference, 74 FORDHAM L. REV. 747, 761 (2005) [hereinafter Solove, Fourth Amendment Codification] (considering Professor Kerr's arguments and finding the judiciary to be better guided in answering to the advancements in technology).

<sup>491.</sup> *Id.* at 761.

<sup>492.</sup> See id. at 762 (answering Professor's Kerr's article and explaining why Congress is not better-suited to respond to growing technological concerns).

<sup>493.</sup> See id. (arguing that destroying the current framework is unnecessary).

<sup>494.</sup> Kerr, The Fourth Amendment, supra note 435, at 871.

<sup>495.</sup> Solove, Fourth Amendment Codification, supra note 490, at 761–73.

<sup>496.</sup> See Kerr, The Fourth Amendment, supra note 435, at 875 (describing the judicial information deficit that can occur as a result of the technological complexities).

knowing more about the policies in play, such as the details of governing law and scope of authority granted to government officials, courts lack the ability to determine whether the violation is an intrusion on an individual and his property interests or an intrusion on an individual's reasonable expectation of privacy in the Fourth Amendment context. 497

A need for a bridge between existing precedent and government transparency exists and can only be brought into fruition through compliance on both ends, from ex post reasoning to observance and compliance with established precedent. While some argue that Congress is more capable of handling developing regulations regarding privacy and surveillance, until Congress moves to step in and regulate behavior in response to advancing technology, established precedent remains the primary barrier to privacy.

#### VI. Conclusion

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," typically factoring in an individual's reasonable expectation of privacy or intrusion on his or her property.<sup>501</sup> Warrants are therefore necessary in almost all

<sup>497.</sup> See Allen Declaration, supra note 17, at 2–3 (mentioning the GPS border policy's existence without discussing the authority or when it was implemented); see also discussions supra Sections II.A, III.B, IV.

<sup>498.</sup> See supra notes 424–496 and accompanying text.

<sup>499.</sup> See Kerr, The Fourth Amendment, supra note 435, at 870, 873, 888 (discussing why legislation is better suited, more expansive, and efficient); see also Orin S. Kerr, Congress, The Courts, and New Technologies: A Response to Professor Solove, 74 FORDHAM L. REV. 779, 780–81 (2005) (critiquing Professor Solove's approach in allowing the judiciary to handle technological advancements).

<sup>500.</sup> See Solove, Fourth Amendment Codification, supra note 490, at 747–48 (arguing that the judiciary is fully capable of handling ensuring that Fourth Amendment protections remain steadfast in the fact of evolving technologies).

<sup>501.</sup> U.S. Const. amend. IV; see, e.g., Katz v. United States, 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring) (developing a subjective and objective test as to whether an individual has a reasonable expectation of privacy); see also United States v. Jones, 565 U.S. 400, 401, 408–11 (2012) (holding "the Katz reasonable-expectation-of-privacy test [] added to, not substituted for, the common-law trespassory test").

instances for a valid search to occur.<sup>502</sup> While the Border Search Doctrine is an exception to this rule meant to protect national sovereignty and the interests of the state,<sup>503</sup> opaque governmental measures and incongruities with Fourth Amendment precedent highlight the potential decline of privacy interests for citizens and non-citizens alike at the border.<sup>504</sup> The GPS border policy promulgated in *United States v. Ignjatov* serves merely as one example of the growing disparity between the scope of Fourth Amendment jurisprudence and the Border Search Doctrine on privacy interests.<sup>505</sup>

A need for greater transparency in enacting policy enforcement measures exists in the Fourth Amendment sphere, and while some may argue for legislators to step in for the courts, courts remain better equipped to develop rules in real-time.<sup>506</sup> However, to ensure transparency, privacy, and trust amongst the citizenry both at and near the border, the government and courts need to work together rather than apart.<sup>507</sup>

<sup>502.</sup> Katz, 389 U.S. at 357 (majority opinion) (noting that warrantless searches are typically unlawful "subject to a few specifically established and well-delineated exceptions").

 $<sup>503.\;\;</sup>See$  United States v. Ramsey, 431 U.S. 606, 616–17 (1977) (highlighting border agent rights).

<sup>504.</sup> See discussion supra Part V.

<sup>505.</sup> See discussion supra Section III.A.

<sup>506.</sup> See discussion supra Part V.

<sup>507.</sup> See discussion supra Part V.