THE "BORDER" OF CONSTITUTIONAL ELECTRONIC PRIVACY RIGHTS: ELECTRONIC SEARCHES AND SEIZURES AT THE UNITED STATES' TERRITORIAL LIMITS

Ryan Garippo[1]

INTRODUCTION

On February 9, 2021, the First Circuit Court of Appeals issued the latest opinion in an ongoing debate amongst the federal circuits.[2] The issue presented was whether it was constitutional for federal agents to search a suspect's electronic device at the United States' border without a warrant. Given the importance of electronic privacy rights in our increasingly digital world, this opinion could have sweeping implications for the future of our constitutional tradition.

In the United States of America, the state is not free to arbitrarily conduct unreasonable searches of the property of its people.[3] This prohibition against unreasonable searches applies to citizens and undocumented immigrants alike.[4] This protection against unreasonable searches is enshrined in the Fourth Amendment of the United States Constitution, which states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[5]

However, this prohibition is not an absolute protection against state-conducted

---

[1] Candidate for Juris Doctor, Notre Dame Law School (2022); Bachelor of Arts in Liberal Arts and Sciences, University of Illinois at Urbana-Champaign (2019). I would like to extend a special thank you to all of my fellow editors on the Notre Dame Journal on Emerging Technologies for their assistance throughout the editing process. I am especially grateful for the never-ending support from my fiancée Elizabeth, my parents, and my siblings. This Note would not have been possible without any of you.

[2] Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021).

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

[4] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 272 (1990) (acknowledging that the Fourth Amendment has previously applied to undocumented immigrants on United States territory and stating that the Supreme Court has never explicitly overturned that precedent).

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

searches of any type.[6] Rather, it is better understood as a prohibition against "unreasonable" state-conducted searches.[7] This is because the Fourth Amendment only applies when a person has a legitimate "reasonable expectation of privacy."[8] Consequently, "reasonableness" has been described as the "ultimate touchstone of the Fourth Amendment."[9]

Under this line of jurisprudence, the Supreme Court has determined "that reasonableness generally requires the obtaining of a judicial warrant."[10] However, the Court has also acknowledged that in certain circumstances, a search may be reasonable without a judicial warrant.[11] The Supreme Court has held that it is generally unreasonable, and thus unconstitutional, for the state to search an individual's electronic device without a warrant.[12] In *Carpenter v. United States*, the Court explained that by allowing the state to search an individual's cell phone without a warrant, it would be providing "an intimate window into a person's life."[13] That window would contain information completely unrelated to the underlying suspected criminal conduct including the individual's "familial, political, professional, religious, and sexual associations."[14] Consequently, the Supreme Court stated that without a warrant, it would be unreasonable to search a person's cell phone.[15]

---

[6] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).
[7] *See* U.S. CONST. amend. IV.
[8] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); Oliver v. United States, 466 U.S. 170, 177 (1984) (using the language of "reasonable expectation of privacy" in the analysis of a majority opinion).
[9] Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006).
[10] Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).
[11] *See* Riley v. California, 573 U.S. 373, 382 (2014).
[12] *See id.* at 386 (declining to extend the search incident to arrest doctrine to cell phones); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured" by a cell phone).
[13] Carpenter, 138 S. Ct. at 2217.
[14] *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
[15] Carpenter, 138 S. Ct. at 2217.

However, there is still some telephone data that the state can obtain without a warrant.[16] In *Smith v. Maryland*, the Supreme Court affirmed the use of the third-party doctrine as it pertains to certain types of data produced by telephones.[17] The third-party doctrine states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to a third party."[18] In *Smith*, a telephone company, at the request of the state, installed a device called a pen register which recorded all the numbers dialed from the defendant's home telephone.[19] The Supreme Court held that the defendant had voluntarily turned over that data to his telephone company and thus he was not entitled to any constitutional protection.[20] In *Carpenter*, the Supreme Court was careful not to overturn *Smith*, stating that there are "limited capabilities" in the type of information obtainable through a pen register.[21] The Supreme Court reasoned that the type of information obtainable through a cell phone search, rather than a simple call-records search provided by a pen register, was far more intrusive and passed the threshold of what is considered reasonable.[22]

This analysis is not unique to electronic data. A similar rationale applies to other Fourth Amendment searches. If the state is unreasonably searching a person's effects, electronic or non-electronic, then it needs a warrant. However, the Supreme Court has been willing to recognize certain historical exceptions to the warrant requirement.[23]

---

[16] *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).
[17] *Id.*
[18] *Id.* at 743–44.
[19] *Id.* at 737.
[20] *Id.* at 745–46.
[21] Carpenter, 138 S. Ct. at 2219.
[22] *Id.*
[23] *See* Riley v. California, 573 U.S. 373, 382 (2014).

One of these exceptions to the warrant requirement is the border search exception.[24] Historically, the executive branch has had the "plenary authority to conduct routine searches at the border, without probable cause or a warrant."[25] These searches are "not subject to any [reasonableness] requirement" including lesser standards than probable cause.[26] Contained within the meaning of the term "routine search" is the authority to "search carry-on bags and checked luggage, conduct canine sniffs or pat-downs, photograph and fingerprint travelers, and even disassemble the gas tank on a vehicle."[27] Historically, this plenary authority to conduct routine searches has been "necessary to prevent smuggling and to prevent prohibited articles from" entering the country.[28]

However, it is important to note that this exception is not all-encompassing and does not necessarily cover nonroutine border searches. Nonroutine border searches include "strip, body cavity, or involuntary x-ray searches."[29] The Supreme Court has suggested that a standard that is less strict than probable cause may be the proper standard for nonroutine searches, although it has declined to decide that officially.[30]

Due to the fact that the stated goal of the border search exception is to prevent smuggling, particularly of prohibited articles, most searches justified under the exception will be physical in nature. For example, if the state is searching an individual for illegal narcotics at the border, it logically follows that the state would

---

[24] United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).
[25] *Id.* at 537.
[26] *Id.* at 538.
[27] Kelly A. Gilmore, *Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border*, 72 BROOK. L. REV. 759, 766–67 (2007).
[28] United States v. 12 200-Foot Reels of Super 8mm. Film, 413 U.S. 123, 125 (1973).
[29] Montoya de Hernandez, 473 U.S at 541 n. 4.
[30] *Id.* at 541–42.

search the physical possessions of an individual to ensure that there are not any narcotics entering the country. Hardly anyone would doubt the constitutionality of this search.

However, it is unclear under what circumstances the border search exception can be used to waive the warrant requirement for electronic devices. On one hand, the state has an interest in preventing illegal articles from entering the country, and evidence of such crimes may be contained on an individual's electronic devices. On the other hand, these devices contain a myriad of personal information in which the state has no legitimate interest to arbitrarily search. This has led courts to distinguish between manual and forensic searches.[31] Manual searches are conducted by a government officer who searches the device by reviewing its contents in a way that any normal user of the device would.[32] In contrast, a forensic search is conducted by computer software which is "capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on websites." [33] Consequently, a forensic search has the capacity to produce much more personal information than a manual search.[34] To this date, no federal circuit court has held that it is ever unconstitutional for the state to manually search an individual's electronic device. However, the same cannot be said for forensic searches.

The constitutional question of when the border search exception can be used to justify a forensic search of an individual's electronic device has proved vexing for

---

[31] *See* United States v. Cotterman, 790 F.3d 952, 967 (9th Cir. 2013) (en banc).
[32] *Id.*
[33] *Id.* at 957.
[34] In its Fourth Amendment jurisprudence, the Supreme Court has been wary of technology which allows officers to conduct searches that they could not otherwise perform using their natural senses alone. This is especially true in the context of technology which is not in general public use. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

courts. Consequently, there is currently a federal circuit split regarding when such searches are proper. The approach taken by the Fourth and Ninth Circuits requires the government to at least have reasonable suspicion before performing a forensic search of an individual's cell phone.[35] Reasonable suspicion is an intermediate standard of review in criminal cases which "is 'considerably less than proof of wrongdoing by a preponderance of the evidence,' and 'obviously less' than is necessary for probable cause."[36] This standard requires only that a government agent have a "particularized and objective basis for suspecting the particular person stopped of criminal activity."[37]

The Eleventh Circuit takes a substantially different approach: it does not require any level of particularized suspicion to be shown for a forensic search of an individual's electronic device to be proper.[38] This approach is extremely deferential to government officers and allows these officers to conduct forensic searches of electronic devices in essentially all circumstances.

In the recent challenge brought before the First Circuit, the court was not required to directly answer what level of particularized suspicion is required for a forensic search.[39] However, its holding is consistent with the jurisprudence set forth by both the Fourth and Eleventh Circuits. Furthermore, it is important to note that there have been legal challenges brought on this issue in the Fifth,[40] Seventh,[41] and Tenth[42] Circuits. However, in each of these cases, the court declined to decide the

---

[35] *See* United States v. Kolsuz, 890 F.3d 133, 148 (4th Cir. 2018); *see also* United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019).
[36] Navarette v. California, 572 U.S. 393, 397 (2014) (quoting United States v. Sokolow, 490 U.S. 1, 7 (1989)).
[37] Navarette, 572 U.S. at 396 (quoting United States v. Cortez, 449 U.S. 411, 417–418 (1981)).
[38] *See* United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018).
[39] Alasaad v. Mayorkas, 988 F.3d 8, 18 (1st Cir. 2021).
[40] United States v. Molina-Isidoro, 884 F.3d 287, 289 (5th Cir. 2018).
[41] United States v. Wanjiku, 919 F.3d 472, 489 (7th Cir. 2019).
[42] United States v. Williams, 942 F.3d 1187, 1190 (10th Cir. 2019).

constitutional question, because in each case, the constitutional question was not outcome determinative for the litigants in question.

This disagreement between the federal circuit courts gives rise to the subject of this Note. This Note will argue that, as a matter of constitutional interpretation, the approach taken by the Eleventh Circuit is the correct approach. However, due to the highly deferential nature of this approach and its potential for abuse, this Note will also argue that Congress should act to create a statutory protection against these invasive searches.

In Part I of this Note, the approach taken by the Fourth and Ninth Circuits will be analyzed alongside the standard of reasonable suspicion. In Part II, the approaches taken by the Eleventh Circuit and First Circuit will in turn be analyzed through a constitutional lens. Additionally, Part II will explain why the approach taken by the Eleventh Circuit has potentially detrimental effects and is ripe for abuse. Part III will outline what meaningful congressional action on this issue could look like. The goal of this exercise will be to create a constitutionally sound framework that protects the electronic privacy rights of all those under the jurisdiction of the United States.

I. THE FOURTH AND NINTH CIRCUIT'S APPROACH

The approaches taken by the Fourth and Ninth Circuits are similar in almost all relevant ways. Both circuits require a finding of reasonable suspicion before determining that a forensic search of an electronic device was constitutional.[43] Although, this approach provides slightly more protection than the approach taken by the Eleventh Circuit, the standard of reasonable suspicion is not substantial enough to

[43] United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); United States v. Cano, 934 F.3d 1002 (9th Cir. 2019).

afford criminal defendants any meaningful protection. This part of the note will analyze the rich caselaw leading to this precedent, and will also describe several relevant policy considerations that come with the standard of reasonable suspicion.

In 2018, the Fourth Circuit held that reasonable suspicion is constitutionally necessary for a forensic search.[44] In *Kolsuz*, a suspect was detained by federal customs agents at an airport in Virginia after attempting to board a flight to Turkey.[45] This suspect was detained because customs agents had discovered parts of a firearm in his luggage.[46] Consequently, the customs agents took possession of the suspect's cell phone (without a warrant to do so) and conducted a month-long forensic analysis of the phone's digital content.[47] This forensic analysis produced a 900-page report which provided sufficient evidence for two criminal charges.[48] One charge was for smuggling firearms and another for an "associated conspiracy."[49] In a pre-trial motion to suppress the evidence obtained from his cell phone, the suspect argued that the forensic search violated the suspect's Fourth Amendment rights.[50] The district court denied this motion and the suspect was ultimately convicted of both charges.[51] The suspect then appealed the result of his suppression motion to the Fourth Circuit.[52]

Judge Harris, writing for the Fourth Circuit, ruled that at least some form of particularized suspicion is required to support a forensic search of an electronic

---

[44] *See* Kolsuz, 890 F.3d at 148.
[45] *Id.* at 136.
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*

device.[53] The Fourth Circuit stated that forensic searches for electronic devices are analogous to nonroutine searches which may occur at the border.[54] Nonroutine searches include "strip, body cavity, or involuntary x-ray searches" for which the standard of review is likely reasonable suspicion.[55] The Fourth Circuit reasoned that a forensic search is similar to a nonroutine search because a "digital device can reveal an unparalleled breadth of private information" just as a nonroutine search is an extremely intrusive search of a suspect's physical privacy.[56] Thus, the standard of reasonable suspicion (at the least) should apply to forensic searches.[57]

After the Fourth Circuit determined that the standard of reasonable suspicion to be the proper standard for this case, the court decided that the customs agents, in this case, had met that standard.[58] The Fourth Circuit stated that the customs agents had a particularized basis to believe that the suspect's phone contained contents of a crime after finding the firearm parts in his luggage.[59] Thus, the court found it reasonable for the customs agents to search the suspect's phone.[60] In dicta, the Fourth Circuit noted that certain circumstances may require a finding of probable cause in order to justify a forensic search; just as is the case with nonroutine searches.[61] However, it was unnecessary for the Fourth Circuit to consider whether such circumstances were implicated in this case because the customs agents acted in good faith and believed

---

[53] *Id.* at 147–48.
[54] Kolsuz, 890 F.3d at 147.
[55] United States v. Montoya de Hernandez, 473 U.S. 531, 541 n. 4 (1985).
[56] Kolsuz, 890 F.3d at 145.
[57] *Id.* at 148.
[58] *Id.*
[59] *Id.* at 141.
[60] *Id.*
[61] *Id.* at 147.

that a warrant was not required.[62] Therefore, in the name of judicial restraint, the Fourth Circuit declined to define the circumstances where a finding of probable cause would be necessary for a forensic search.[63]

Similarly, in *United States v. Cano*, the Ninth Circuit also held that reasonable suspicion was necessary to justify a forensic search of an individual's electronic device at the border.[64] In *Cano*, the criminal defendant worked in the United States but lived in Mexico.[65] One day when the defendant entered the United States for work, he was stopped in his car by customs agents for a random inspection.[66] During this inspection, authorities searched the defendant's car with a narcotic-detecting dog.[67] The dog directed the authorities to the defendant's spare tire, where they discovered over fourteen kilograms of cocaine.[68] The customs agents manually searched the defendant's cell phone, obtaining the phone numbers of individuals the defendant had called alongside copies of the defendant's text messages.[69] Customs agents then conducted a forensic search of the defendant's phone which granted comprehensive access to the defendant's "text messages, contacts, call logs, media, and application data."[70] Both searches were conducted without warrants.[71] The information contained on the defendant's phone, coupled with the presence of illegal narcotics were sufficient to support a criminal indictment for importing cocaine.[72]

---

[62] *Id.* at 148.
[63] *See id.* at 148.
[64] United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019).
[65] *Id.* at 1008.
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.* at 1008–09.
[71] Cano, 934 F.3d at 1010.
[72] *Id.* at 1009.

Before trial, the defendant filed a motion to suppress the evidence obtained from his cell phone on the grounds that the forensic search violated the Fourth Amendment.[73] The district court denied his motion and held that the evidence from the forensic search was admissible, and the defendant's case proceeded to trial.[74] The defendant's first trial concluded with a hung jury, resulting in an order for a second trial.[75] The second trial resulted in the defendant's conviction.[76] The defendant appealed his case to the Ninth Circuit on the grounds that the warrantless search of his phone violated the Fourth Amendment.[77]

Judge Bybee, writing for the Ninth Circuit, held that reasonable suspicion is necessary to justify a forensic search of an electronic device at the border.[78] The Ninth Circuit stated that a manual search of a cell phone was "a quick look and [an] unintrusive search."[79] Thus, manual searches are always permissible at the border. Conversely, the opinion reasoned that a forensic search of an electronic device would reveal "the most intimate details" of a persons' life, and consequently this data carries a "significant expectation of privacy."[80] The Ninth Circuit analogized an electronic search of this nature to a nonroutine virtual "strip search" at the border.[81] However, the Ninth Circuit also explained that forensic searches do not rise to the level of probable cause because an individual's expectation of privacy is still diminished at the

---

[73] *Id.*
[74] *Id.* at 1009–10.
[75] *Id.* at 1010.
[76] *Id.*
[77] *Id.*
[78] *Id.* at 1016.
[79] *See id.* at 1015 (quoting United States v. Cotterman, 790 F.3d 952, 960-61, 966, 967 (9th Cir. 2013) (en banc)).
[80] United States v. Cano, 934 F.3d 1002, 1015 (9th Cir. 2019) (quoting United States v. Cotterman, 790 F.3d 952, 965–66 (9th Cir. 2013) (en banc)).
[81] Cano, 934 F.3d at 1015 (quoting *Cotterman*, 790 F.3d at 960-61, 966, 967).

border.[82] Therefore, the Ninth Circuit concluded that reasonable suspicion is the proper standard under which to analyze forensic search cases.

The Ninth Circuit also added an additional constraint to the reasonable suspicion doctrine.[83] The Ninth Circuit held that a forensic search must be limited to actual contraband instead of just mere evidence of a crime.[84] This is because "[b]order officials are authorized to seize 'merchandise which. . . . [has] been introduced into the United States in any manner contrary to law."[85] The court held that the term merchandise was limited to illegal contraband as opposed to any evidence that a crime occurred.[86] For example, a customs agent could seize child pornography if it was found in a forensic search because child pornography is categorized as illegal contraband in the United States.[87] However, under this standard, a customs agent could not seize text messages which indicated an ongoing conspiracy because text messages, on their own, do not qualify as contraband.[88] The Ninth Circuit reasoned that this requirement was proper because the border search exception is justified in preventing illegal articles from crossing our border.[89] The exception was not meant to serve as a "general authority to search for crime" of any type.[90] Note that the Ninth Circuit acknowledged its slight disagreement with the Fourth Circuit, which had not attempted to draw this additional requirement.

A. An Analysis of The Reasonable Suspicion Doctrine

---

[82] *See* Cano, 934 F.3d at 1015–16.
[83] *Id.* at 1018.
[84] *Id.*
[85] *Id.* at 1017 (quoting 19 U.S.C. § 482(a)).
[86] *See* Cano, 934 F.3d at 1017.
[87] *See id.*
[88] *See id.*
[89] *See id.* at 1018.
[90] *Id.* at 1017.

The Fourth and Ninth Circuits have both adopted some variation of the reasonable suspicion standard for electronic border searches. However, it is worth noting that the "reasonable suspicion" standard has not been without controversy since its emergence in the landmark case of *Terry v. Ohio*.[91] If reasonable suspicion applies, the state actor is only required to have a "particularized and objective basis for suspecting the particular person stopped of criminal activity" before conducting a limited search.[92] This totality of the circumstances standard has been criticized by many, including textualists,[93] constitutional historians[94], and those concerned with the practical policy considerations that this doctrine creates.[95] Although the doctrine is not without its benefits, these critiques, when leveraged together, make a compelling case against the doctrine.

The textual argument against the reasonable suspicion doctrine is quite strong because illogical interpretive issues arise when the two clauses of the Fourth Amendment, the "unreasonable search clause" and "warrant clause," are read separately.[96] The "unreasonable search clause" of the Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[97] In turn, the "warrant clause" states that "no Warrants shall issue, but upon probable cause,

---

[91] Terry v. Ohio, 392 U.S. 1, 37 (1968) (Douglas, J., dissenting).
[92] Navarette v. California, 572 U.S. 393, 396 (2014) (quoting United States v. Cortez, 449 U.S. 411, 417–418 (1981)).
[93] *See* Esther Jeanette Windmueller, *Reasonable Articulable Suspicion – The Demise of Terry v. Ohio and Individualized Suspicion*, 25 U. RICH. L. REV. 543, 545–546 (1991).
[94] *See id.*
[95] *See* Randall S. Susskind, *Race, Reasonable Articulable Suspicion, and Seizure*, 31 AM. CRIM. L. REV. 327, 332 (1994).
[96] Windmuller, *supra* note 93, at 545–46.
[97] U.S. CONST. amend. IV.

supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."[98] These two clauses are joined by a conjunction.[99] That conjunction is the word "and."[100]

According to Esther Windmueller, much of the academic debate surrounding the Fourth Amendment concerns this conjunction.[101] This is because there are multiple possible interpretations of this conjunction and each interpretation produces a different result.[102] To explain the distinctions between these interpretations, Windmueller quotes Professor Jacob Landynski to demonstrate that the conjunction can lead to three reasonable interpretations:

> (1) that the "reasonable" search is one which meets the warrant requirements specified in the second clause;
> (2) that the first clause provides an additional restriction by implying that some searches may be "unreasonable" and therefore not permissible, even when made under a warrant; or
> (3) that the first clause provides an additional search power, authorizing the judiciary to find some searches "reasonable" even when carried out *without* warrant.[103]

The importance of this interpretive issue cannot be understated. The reasonable suspicion doctrine is justifiable only under Professor Landynski's third possible interpretation,[104] but the third interpretation produces results that are inconsistent with a logical reading of the Constitution.

It is a common rule of textual interpretation that the text of statutes or the

---

[98] *Id.*
[99] *See id.*
[100] *Id.*
[101] Windmuller, *supra* note 93, at 545–46.
[102] *See id.* at 546.
[103] *Id.* (citing J. Landynski, SEARCH AND SEIZURE AND THE SUPREME COURT: A STUDY IN CONSTITUTIONAL INTERPRETATION 42–43 (1966) (emphasis in original)).
[104] Landysnki, *supra* note 103, at 43, (explaining that although the third interpretation may be possible from the grammatical standpoint, it is not a valid option amongst other interpretations because it is not consistent without the historical intent of the founders).

Constitution should not be read in such a way to produce an "absurd" result.[105] The third interpretation of the Fourth Amendment produces exactly such a result. As Justice Douglas noted in his dissent in *Terry*, the third interpretation of the Fourth Amendment grants more authority to police officers and other state officials than to courts.[106] This is because, under a reasonable suspicion analysis, a state official is empowered to conduct a search once he has a particularized basis for believing a suspect is engaged in criminal activity. If this state official can articulate a reasonable basis for his suspicion in court, then courts are obligated to uphold the search. Conversely, under a probable cause standard, police officers and other state actors are required to seek a warrant from a judicial magistrate unless there are exigent circumstances present.[107] However, the judicial magistrate is only empowered to authorize a search upon a finding of probable cause.[108] As previously noted, reasonable suspicion is a significantly less demanding standard than probable cause.[109] As a result, under the third interpretation, police officers and other state actors have more authority to authorize a search than a judicial magistrate.

It would be an absurd result to continue to recognize this interpretation because it completely eviscerates the need for probable cause and warrants when searching a

---

[105] *See* United States v. Providence Journal Co., 485 U.S. 693, 710 (1988) (Stevens, J., dissenting) (explaining that the Supreme Court has "long held that in construing a statute, we are not bound to follow the literal language of the statute—however clear the words may appear on 'superficial examination'—when doing so leads to 'absurd,' or even 'unreasonable,' results." (quoting United States v. American Trucking Assns., Inc., 310 U.S. 534, 543–44 (1940) (internal quotation marks and citation omitted.)).

[106] Terry v. Ohio, 392 U.S. 1, 36 (1968) (Douglas, J., dissenting).

[107] Carpenter v. United States, 138 S.Ct. 2206, 2222–23 (2018).

[108] *See* Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (explaining that "[p]robable cause exists where 'the facts and circumstances within. . . . [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed."

[109] *See* Navarette v. California, 572 U.S. 393, 397 (2014).

suspect. If an officer can conduct a search without a warrant, under a lesser standard of scrutiny, then there is no logical reason to consult a judicial magistrate. Although searches under reasonable suspicion must be limited in nature, if an officer acquires probable cause within the course of his search, then the officer is permitted to conduct a full search under that doctrine. Consequently, the third interpretation and the reasonable suspicion doctrine can effectively operate as a means of completely bypassing the initial judicial review. The Constitution's framers explicitly recognized the phrase "probable cause" in the Fourth Amendment's text but declined to include the phrase "reasonable suspicion".[110] It is unlikely that the framers would have envisioned a doctrine such as reasonable suspicion, which was not explicitly recognized, to circumvent textual provisions.[111]

Any historical analysis of the Fourth Amendment will also reveal that reasonable suspicion does not comport with an originalist understanding of the Constitution.[112] After all, the British Crown's general search warrant power was one of the main problems that the framers sought to address via the Fourth Amendment.[113] Under British rule, soldiers were free to search the colonists at any point because "officers of the customs [were] empowered to break open and enter houses, without the authority of a civil magistrate, founded on legal information."[114] This led to a host

---

[110] *See* U.S. CONST. amend. IV.
[111] *See* Whitman v. American Trucking Ass'ns., Inc., 531 U.S. 457, 468 (2001) (explaining that when conducting a textual analysis, courts will not construe a vague provision to completely alter the text's meaning because the writers of those provisions would not "hide elephants in mouseholes").
[112] *See* Wyoming v. Houghton, 526 U.S. 295, 299 (1999) (explaining that the necessary first inquiry in any Fourth Amendment case is a historical analysis to determine whether an action was an unlawful search or seizure at the time of ratification).
[113] Martin Grayson, *The Warrant Clause in Historical Context*, 14 AM. J. CRIM. L. 107, 108-117 (1986).
[114] THE FIRST CONT'L CONG., PETITION TO KING GEORGE III (1774).

of abuses by the Crown.[115] These abuses even included instances where British officers would invade any private premise that they desired and seize able-bodied men for military service.[116] These practices were particularly troubling to the colonists because there was a prohibition against such general warrants for British citizens living in England.[117] The logic against this practice was that searches and seizures, without evidence of suspicion, were contrary to the dignity of Englishmen.[118] Additionally, the prohibition served as a check on royal power.[119] Consequently, the framers sought to take advantage of this same protection when they drafted the Constitution.[120]

With this history in mind, it is clear that the framers did not intend to write an additional search power based on "reasonable suspicion" into the Constitution. If the goal of the Fourth Amendment were to provide a check on executive power, it would make no sense to give the executive branch more power to conduct searches than a judicial magistrate. Additionally, there is evidence that the original draft of the Fourth Amendment did not include the illusory conjunction "and," meaning that the third possible interpretation would be eliminated altogether.[121] In fact, this original version of the Fourth Amendment was actually the version that was approved by the Continental Congress, but the current version was only submitted to the states by mistake.[122] Although it is true that the states did not ratify this original draft of the

---

[115] *See* Leonard W. Levy, *Origins of the Fourth Amendment*, 114 POL. SCI. Q. 79, 81-84 (1991).
[116] *See id.* at 83.
[117] *See* Grayson, *supra* note 113, at 112.
[118] *See id.* at 111–12.
[119] *See id.* at 112.
[120] *See id.* at 115–17.
[121] *See id.* at 116–17.
[122] *Id.* at 117.

Amendment, this fact demonstrates that the framers' intent was not to include an additional search power.[123]

In modern practice, those concerned with the practical effects of reasonable suspicion, argue that the doctrine is too broad to meaningfully confine state actors. This critique is particularly salient when one considers the type of actions that often justify a search based on reasonable suspicion. For example, many courts have held a police officer observing a suspect making "furtive movements" is sufficient to satisfy the reasonable suspicion standard.[124] The definition of "furtive movements" is elusive and thus grants substantial deference to police officers. In a 2013 case, *Floyd v. City of New York*, one police officer testified as to his definition of "furtive movements" and stated that:

> "[F]uritve movements is a very broad concept," and could include a person "changing direction," "walking in a certain way," "[a]cting a little suspicious" "making a movement that is not regular," being "very fidgety," "going in and out of his pocket," "going in and out of a location," "looking back and forth constantly," "looking over their shoulder," "adjusting their hip or their belt," "moving in and out of a car too quickly," "[t]urning a part of their body away from you," "[g]rabbing at a certain pocket or something at their waist," "getting a little nervous, maybe shaking," and "stutter[ing]."[125]

This quote is quite illuminating. Under this standard, state officials can conduct searches simply by observing a criminal defendant "looking over their shoulder" and then testifying that they observed "furtive movements."[126] This example shows that far too much innocuous conduct is included under the reasonable suspicion doctrine

---

[123] *See* Grayson, *supra* note 113, at 117.
[124] *See* United States v. Paulino, 850 F.2d 93, 98 (2d Cir. 1988); *see also* United States v. Bullock, 510 F.3d 342, 348 (D.C. Cir. 2007); *see also* United States v. DeJear, 552 F.3d 1196, 1201 (10th Cir. 2009).
[125] *See* Floyd v. City of New York, 959 F. Supp. 2d 540, 561 (S.D.N.Y. 2013); *see also* 5-4, *Terry v. Ohio,* PROLOGUE PROJECTS, (Mar. 24, 2020), https://podcasts.apple.com/us/podcast/5-4/id1497785843?i=1000469323083.
[126] Floyd, 959 F. Supp. 2d at 559.

and that state officials can justify nearly any search under its reach. Because the original intent of the Fourth Amendment was to protect against general arbitrary state conducted searches, reasonable suspicion does not nearly come close to effectuating the founders' intent.

In the context of electronic border searches, it is worth questioning whether this doctrine provides any meaningful protection to criminal suspects. Undoubtedly, the Fourth and Ninth Circuits were hesitant to establish a rule where state officials had no restraints on the circumstances when an electronic forensic search was proper. Consequently, these federal circuits sought to recognize some constitutional protection for criminal suspects. However, these circuits' reliance on the reasonable suspicion doctrine was misplaced. The above example of "furtive movements" highlights this fact.[127] With a standard that is so deferential and broad, a state-conducted search of a suspect's electronic device will nearly always be justified. Because of this fact, the reasonable suspicion doctrine is a less than ideal solution to protect criminal defendants' electronic privacy rights.

Although the reasonable suspicion doctrine is often critiqued, it does provide some useful policy benefits. Many of these benefits come in the form of increased safety for state officials. This is because the original application of the reasonable suspicion doctrine limited such searches to physical "frisks" of suspects for weapons.[128] The rationale was that, when talking to a suspect, a police officer does

[127] Paulino, 850 F.2d at 98.
[128] *See* Terry v. Ohio, 392 U.S. 1, 23 (1968) (noting that the main purpose of a search based reasonable suspicion is for a police officer to "assure himself that the person with whom he is dealing is not armed with a weapon that could unexpectedly and fatally be used against him").

not know whether or not that suspect is armed.[129] Consequently, the Supreme Court stated that it was reasonable for a police officer, in the interest of his own safety, to conduct a limited search of a suspect when he believes he is dealing with an armed and dangerous individual.[130] Since the Supreme Court's decision in *Terry*, these searches have led to countless amounts of illegal weapons being uncovered, which but for their discovery, may have ultimately been used against police officers. Consequently, it is not surprising that advocates of the reasonable suspicion doctrine continue to justify its usefulness on the grounds of officer safety.

While this policy benefit continues to hold weight with respect to physical searches, it is not particularly persuasive in the context of electronic border searches. It is unlikely that a cell phone or electronic device could be used to physically harm an officer. These devices do not present the intrinsic risk of danger that a weapon such as a firearm presents. Furthermore, even if these devices were capable of harming an officer, it is unlikely that a look into the "intimate window" of an individual's personal life would ensure the officer's safety any further.[131] Consequently, the same policy considerations which help justify the reasonable suspicion doctrine for physical searches, do not help justify searches in the electronic context.

For the above reasons, it is likely that the doctrine of reasonable suspicion is constitutionally suspect. Therefore, it is unlikely that the founders would have intended for warrantless electronic searches to be based on this doctrine. The text and history of the Fourth Amendment reveal that the founders likely did not intend for any

---

[129] *See id.* at 23–24.
[130] *See id.* at 27.
[131] *See* Riley v. California, 573 U.S. 373, 382 (2014).

searches to be based solely on reasonable suspicion, a fact which may be persuasive to the Supreme Court, given its current composition of predominately originalist justices. The founders likely viewed the Fourth Amendment in a much simpler way.[132] Under this alternative view of the Fourth Amendment, a state official either needed to have a warrant or needed to be able to justify their search under a well-established exception.[133] Therefore, should the Supreme Court choose to grant a writ of certiorari on this issue, it may be prudent for the Court to revisit its reasonable suspicion jurisprudence in its entirety.

Based on this analysis, it is unlikely that forensic searches of electronic devices at the border are subject to the reasonable suspicion doctrine. There are strong textual and historical arguments against the doctrine in its entirety. As applied to the context of electronic searches at the border, this doctrine fails to meaningfully protect criminal defendants and obtain the typical policy benefits that come from the continued existence of the doctrine for physical searches. Therefore, the reasonable suspicion doctrine is not the proper standard to analyze cases that involve electronic searches at our nation's border.

II. THE ELEVENTH AND FIRST CIRCUIT'S APPROACH

The Eleventh Circuit takes an approach that differs from the Fourth and Ninth Circuits. The Eleventh Circuit has held that there is no level of particularized suspicion required to conduct an electronic forensic search at the border.[134] By taking this approach, the functional implication is that state officials can search anyone's

[132] *See* Landysnki, *supra* note 103, at 42–43.
[133] *See id.*
[134] *See* United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

electronic device at the United States' border without providing any justification. Although this approach is more consistent with the historical tradition of the Constitution, it carries with it a high potential for abuse. This part of the note will analyze the case law which created this precedent and will also describe the ways that this approach could be abused.

The Eleventh Circuit's electronic border search framework is contained its 2018 decision titled *United States v. Touset*.[135] In *Touset*, a criminal defendant was searched at an Atlanta airport while preparing to board an international flight.[136] In the years prior to his search, the defendant had been under investigation by several private organizations and the federal government for suspected child pornography transportation.[137] Consequently, when the defendant attempted to board an international flight, the customs agents initiated a search of the defendant's electronic devices.[138] In his possession, the defendant had "two iPhones, a camera, two laptops, two external hard drives, and two tablets."[139] The customs agents conducted a manual search of the defendant's camera and iPhones.[140] Neither device contained any child pornography and consequently, the devices were returned to the defendant.[141] However, the customs agents detained the remaining electronic devices for a forensic search.[142] The forensic search revealed child pornography on the defendant's laptops and hard drives.[143]

---

[135] *Id.* at 1229.
[136] *Id.* at 1230.
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*.

Using this evidence, the government was able to obtain a search warrant for the defendant's Georgia home.[144] As a result of this investigation and search, the government discovered that the defendant had "sent more than $55,000 to the Philippines for pornographic pictures, videos, and webcam sessions" with children.[145] Additionally, the agents discovered that the defendant also "created an Excel spreadsheet that documented the names, ages, and birthdates of those young girls as well as his notes about them."[146] While searching the defendant's home, the customs agents also interviewed the defendant and placed him under arrest.[147]

In a pre-trial motion, the defendant argued that the initial forensic search of his laptops and hard drives violated the Fourth Amendment.[148] The defendant also argued that the rest of the evidence obtained at his home should be suppressed as the fruit of the poisonous tree.[149] The district court ruled against the defendant's motion and adopted the Ninth Circuit's approach towards reasonable suspicion set forth in *Cotterman*.[150] Subsequently, the defendant pled guilty to his charges but reserved the right to appeal the result of his suppression motion.[151] Consequently, after the defendant received a sentence of 120 months of imprisonment and supervision for life, he appealed the result of his suppression motion to the Eleventh Circuit.[152]

Judge Pryor, writing for the Eleventh Circuit, stated that there is no level of particularized suspicion required to search a suspect's electronic device at the

---

[144] *Id.*
[145] *Id.*
[146] *Id.* at 1230–31.
[147] *Id.* at 1230.
[148] *Id.* at 1231.
[149] *Id.*
[150] *Id.*
[151] *Id.*
[152] *Id.*

border.[153] The Eleventh Circuit quoted Supreme Court precedent that stated "searches at the border of the country 'never require probable cause or a warrant.'"[154] This is because the government has broad powers at the border to "prevent smuggling and prevent prohibited articles from entry."[155] According to the Eleventh Circuit, these broad powers grant the federal government the authority to search any form of property that is crossing the nation's border.[156] The court went on to state that, as early as the First Congress, government officials had been empowered to search the property of any "vessel" without a warrant.[157] This power applied not only at points of entry but also "before [the vessels even] reached the United States."[158] The Eleventh Circuit used this evidence to conclude that searches of property at the border were not included within the original public meaning of the Fourth Amendment.[159]

Although, the Eleventh Circuit did note that if the state conducted certain types of invasive searches of a person, then the standard of reasonable suspicion may apply, but it declined to extend that standard to any form of property.[160] The Eleventh Circuit also stated that there is nothing that prevents "Congress from enacting laws that provide greater protections than the Fourth Amendment requires."[161] However, absent such legislation, the Eleventh Circuit held that forensic searches of electronic devices are constitutional because such devices are a quintessential form of personal

---

[153] *Id.* at 1231–32.
[154] *Id.* at 1232 (quoting United States v. Ramsey, 431 U.S. 606, 619 (1977)).
[155] United States v. 12 200-Foot Reels of Super 8mm. Film, 413 U.S. 123, 125 (1973).
[156] Touset, 890 F.3d at 1233.
[157] *Id.*
[158] *Id.*
[159] *Id.* at 1231–32.
[160] *Id.* at 1233.
[161] *Id.* at 1236.

property.[162]

However, it is also worth noting that the Eleventh Circuit's Fourth Amendment analysis in *Touset* may have been dicta. This is because the Eleventh Circuit also affirmed the district court's finding of reasonable suspicion.[163] The Eleventh Circuit reached this conclusion because the criminal defendant had sent three low-value money transfers to a suspicious financial account prior to his search.[164] This financial account was suspicious because of the phone number registered to the account.[165] That phone number had also been registered to an email address that previously had been discovered to contain child pornography.[166] Additionally, the Eleventh Circuit noted that "a pattern of 'frequent low money transfers' is associated with child pornography."[167] It was this pattern combined with the fact that the defendant was carrying nine different electronic devices which led the Eleventh Circuit to conclude reasonable suspicion was present in this case.[168]

Therefore, because the Eleventh Circuit's Fourth Amendment jurisprudence was not outcome determinative to the *Touset* case, it was likely dicta. Multiple other federal circuit courts, when faced with this same set of circumstances, have declined to decide the issue.[169] This is indicative of the fact that the Eleventh Circuit analysis was likely dicta. However, it is likely that the Eleventh Circuit will continue to decide cases using this framework because it strongly condemned the use of the reasonable

---

[162] *Id.* at 1233.
[163] *Id.* at 1237.
[164] *Id.*
[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] *See* United States v. Molina-Isidoro, 884 F.3d 287, 289 (5th Cir. 2018); *see also* United States v. Wanjiku, 919 F.3d 472, 489 (7th Cir. 2019); *see also* United States v. Williams, 942 F.3d 1187, 1190 (10th Cir. 2019).

suspicion doctrine in cases where electronic devices were searched at the border.

In the most recent case on the subject, the First Circuit took an approach that is quite similar to the approach taken by the Eleventh Circuit.[170] In *Alasaad*, the First Circuit considered the first civil case to challenge the border search exception as applied to electronic devices.[171] The plaintiffs were ten United States citizens and one lawful permanent resident, each of whom had their electronic devices searched by federal border agents.[172] Each of these plaintiffs had their electronic devices searched under the same policy set forth by the federal government.[173] Namely, that policy permitted federal agents to manually search electronic devices with no level of individualized suspicion or forensically search a device with reasonable suspicion.[174] It is important to note that the plaintiffs did not contend that the federal agents had violated their policies, but rather that the policy itself was unconstitutional.[175] Accordingly, these plaintiffs, with the help of the American Civil Liberties Union, brought suit seeking to enjoin the federal government from continuing this policy.[176]

Judge Lynch, writing for the First Circuit, held that neither the federal government's policy for manual searches nor forensic searches were unconstitutional.[177] With respect to the manual search standard, the First Circuit agreed with all the other federal circuits to consider this issue to date, holding that no level of individualized suspicion is required for a manual search to occur.[178] The First

[170] Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021).
[171] *Id*. at 13.
[172] *Id.* at 14.
[173] *Id.* at 13–14.
[174] *Id*.
[175] *Id.* at 16–21.
[176] *Id.* at 12.
[177] *Id.* at 12–13.
[178] *Id.* at 18–19.

Circuit stated that although manual "[e]lectronic device searches do not fit neatly into other categories of property searches . . . the bottom line is that basic border searches of electronic devices do not involve an intrusive search of a person" and thus are constitutional.[179]

However, with respect to the forensic search policy, the First Circuit took an approach that distinguished it from some of the other federal circuits. This holding has two parts; the level of individualized suspicion required and the scope of the search power.[180] Regarding the first part, the First Circuit held that a finding of probable cause is not required for forensic searches at the border.[181] This is consistent with every other federal circuit to consider this issue to date and is not where this case is differentiable. Based on the facts of this civil case, the First Circuit was not asked to consider whether reasonable suspicion is required for a forensic search, because the plaintiffs did not challenge whether the officers had reasonable suspicion. Therefore, it is still an open question whether any level of particularized suspicion is necessary for a forensic search to be conducted at the border.

The point where the First Circuit's holding is differentiable is the scope of the doctrine. The First Circuit explicitly rejected the Ninth Circuit's approach and held that forensic searches are not limited only to searches for contraband.[182] The First Circuit states that "the border search exception's purpose is not limited to interdicting contraband; it serves to bar entry to those 'who may bring anything harmful into this

[179] *Id.* at 18.
[180] *Id.* at 19–21.
[181] *Id.* at 12.
[182] *Id.* at 19-20.

country.'"[183] The First Circuit explains that this rationale governs "whether that [thing] be communicable diseases, narcotics, or explosives."[184] Furthermore, the First Circuit notes that Congress is in a better position than the courts to identify harms at the border and invited legislation that would extend protections to those traveling beyond the United States' territorial limits.[185] However, absent such legislation, the First Circuit held that the information obtained in a constitutional forensic search need not be subjected to a contraband requirement.[186]

Additionally, it is worth noting that the First Circuit's approach is completely consistent with the Eleventh Circuit and Fourth Circuit's approaches. All of these circuits have held that no level of particularized suspicion is required for a manual search. Additionally, all of these circuits have held that there is no contraband requirement for forensic searches. The key point where the Fourth and Eleventh Circuit differ is on whether reasonable suspicion is required at all. As was previously noted, this is not a question that the First Circuit was required to answer. Although, insofar as the First Circuit has not answered this question, its holding remains consistent with the jurisprudence from the Fourth and Eleventh Circuits.

Based on the holding in *Alasaad*, it would not be surprising if the First Circuit ultimately decides that no level of particularized suspicion is required for forensic searches at the border. This is because the Eleventh Circuit's Fourth Amendment analysis is quite strong. If governmental officials have historically been able to search any form of personal property at the border, then it stands to reason that the same rule

---

[183] *Id.* at 20 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 544 (1985)).
[184] *Id.*(quoting Montoya de Hernandez, 473 U.S. at 544).
[185] *Id*.
[186] *Id.*

should apply to electronic devices. Prior to the invention of electronic devices, physical searches of personal property could still provide "an intimate window into a person's life."[187] For example, imagine a physical search at the border of a criminal suspect's private journal. Such a search would be undoubtedly constitutional and may easily provide the same private information that an individual may keep on his electronic device. This makes the Ninth Circuit's description of electronic border searches as a type of virtual strip search seem a bit exaggerated as we would never describe a physical search of a journal in such a way.[188] The Constitution permits the federal government to have broad discretion when initiating searches of property at our nation's border. This broad discretion includes forensic searches of electronic devices under its scope.

There are those who would take exception to this analogy. Critics of this approach would say that a physical search of a journal is akin to a manual search at the border as opposed to a forensic one. This is because there is no highly specialized technology required to manually search a defendant's journal, but such technology is required to conduct a forensic search of a suspect's electronic device. The Supreme Court has a longstanding skepticism against warrantless searches conducted using highly specialized technology; an argument which is now being deployed in the context of the border exception.

The crux of this argument comes from a seminal case in Fourth Amendment jurisprudence, *Kyllo v. United States.*[189] In *Kyllo,* federal agents suspected a criminal

[187] Carpenter v. United States, 138 S.Ct. 2206, 2217 (2018).
[188] United States v. Cano, 934 F.3d 1002, 1015 (9th Cir. 2019).
[189] 533 U.S. 27 (2001).

defendant of growing marijuana in his home.[190] Knowing that marijuana typically requires high-intensity heat lamps to grow, the agents conducted a heat-sensing thermal imaging scan of the defendant's home from across the street.[191] The agents did not have a warrant prior to conducting this scan.[192] The scan revealed high levels of heat radiation which were "not visible to the naked eye."[193] The agents used this information to then secure a judicial search warrant which they used to search the premises.[194] The search revealed over one hundred marijuana plants and the defendant was subsequently charged with manufacturing marijuana.[195]

Subsequently, the defendant argued that the thermal scan of his home was unconstitutional under the Fourth Amendment.[196] The defendant argued that he had a reasonable expectation of privacy in his home and that it was not reasonable for the agents to defeat that expectation of privacy using a thermal imaging device.[197] Justice Scalia, writing for the majority, agreed with the defendant's argument.[198] The Court reasoned that using sense-enhancing technology to obtain "any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'. . . constitutes a search – at least where (as here) the technology in question is not in general public use."[199] The thermal imaging device was not in general public use and the home is a constitutionally

---

[190] *Id.* at 29.
[191] *Id*29–30.
[192] *See id.*
[193] *Id.* at 29.
[194] *Id.* at 30.
[195]*Id*.
[196] *See id.* at 33–34.
[197] *Id.* at 34–35.
[198] *Id.* at 40.
[199] *Id.* at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

protected area. Therefore, the agents would have either needed probable cause or a warrant from a judicial magistrate in order to permissibly conduct the thermal imaging scan.

Those who disagree with the Eleventh Circuit's approach in *Touset* make a similar argument.[200] These critics argue that the Supreme Court precedent in *Riley* established that criminal defendants have a reasonable expectation of privacy in their cell phones.[201] This is similar to the reasonable expectation of privacy that the defendant in *Kyllo* had in his home.[202] The argument then follows that forensic searches of electronic devices are akin to thermal imaging scans because each requires highly specialized technology which is not available to the general public. Consequently, these critics conclude that forensic searches at the border are a type of unreasonable search.

However, the faith that these critics place in *Kyllo*'s holding is misplaced. This is because *Kyllo* is distinguishable in one fundamental way. *Kyllo* did not occur at the border, it occurred at the defendant's home.[203] Hardly any constitutional scholar would argue that a warrantless forensic search of a defendant's cell phone would be constitutional within the nation's interior. However, as has been demonstrated previously, there are a variety of searches that are constitutional at the nation's border that are unconstitutional in the nation's interior.[204] As the Eleventh Circuit explained, forensic searches of electronic devices are included in this category and are thus

---

[200] United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018).
[201] Riley v. California, 573 U.S. 373, 382 (2014).
[202] *See* Kyllo 533 U.S. at 33–34.
[203] *Id.* at 29.
[204] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

constitutional.

Additionally, it is worth noting that the arguments made against the constitutionality of reasonable suspicion are also consistent with the Eleventh Circuit's interpretation. As was explained in the previous section, the founders likely viewed the probable cause requirement as a binary distinction. Before conducting a search, state actors either needed to have probable cause or to be covered by a historical exception, otherwise, the search was unconstitutional. To this date, not a single United States circuit court has held that probable cause is required to conduct a forensic search at the border. This is because every federal circuit court recognizes the federal government has the plenary power to control our nation's borders which creates a diminished expectation of privacy for criminal defendants. This plenary power would still exist, even if the standard of reasonable suspicion were not available within criminal law. If one subscribes to the arguments against the reasonable suspicion doctrine, the only thing left to decide is whether electronic device searches fall under the scope of the border exception, a question which has been answered in the affirmative by every United States circuit court to analyze this issue thus far. Consequently, the original public meaning of the Fourth Amendment does allow for forensic searches of electronic devices at the nation's border.

Although the original public meaning of the Fourth Amendment allows for searches of electronic devices at the border, the concerns of the Fourth and Ninth Circuits are not unfounded. As the Ninth Circuit noted in the recent case, *United States v. Moalin*, the federal government has increasingly obtained its citizens'

electronic data via a variety of information collection methods.[205] The government's increased possession of its citizens' personal electronic information is a cause for concern. This form of government surveillance gives the federal government access to a large amount of non-illegal personal information and actively undermines the basic principles of a free autonomous society. If the federal government is permitted to search electronic devices at the border without any level of particularized suspicion, then another avenue has been opened for the federal government to obtain private information about its citizens. This could lead to many of the same problems regarding arbitrary searches and seizures which concerned the founders.

However, the Eleventh Circuit's interpretation of the Constitution has practical benefits as well. The most salient of these benefits is the increased ability of federal agents to protect national security at the border. As the Supreme Court recently stated, "one of [the U.S. Customs and Border Protection Agency's] main responsibilities is to 'detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States.'"[206] It is considerably easier for customs agents to "respond to" those "who may undermine the security of the United States," if the agents have the complete authority to search anyone of whom they are suspicious.[207] This may result in the federal government successfully prosecuting more firearm traffickers,[208] drug traffickers,[209] and child pornography distributors.[210] If these criminal offenders can be

[205] 973 F.3d 977, 988–89 (9th Cir. 2020).
[206] Hernandez v. Mesa, 140 S.Ct. 735, 746 (2020) (quoting 6 U.S.C. § 211(c)(5)).
[207] 6 U.S.C. §211(c)(5).
[208] *See* United States v. Kolsuz, 890 F.3d 133, 136 (4th Cir. 2018).
[209] *See* United States v. Cano, 934 F.3d 1002, 1009 (9th Cir. 2019).
[210] *See* United States v. Touset, 890 F.3d 1227, 1230 (11th Cir. 2018).

searched and arrested at the border, the interior of the United States will likely be safer without these offenders at large.

The national security policy justification is not without merit, as such an approach may result in more criminals being arrested. However, proponents of this approach often overlook the collateral consequences of its implementation. Under this approach, it is just as likely that federal agents will search people who have not committed any criminal offenses as it is that these agents will search criminals. These people, who have not committed any crimes, and despite following all the laws of the United States, may have their phones searched for no reason. These searches will not produce any arrests, nor will the interior of America be any safer. Rather, the foreseeable consequence is that completely innocent Americans will further lose their electronic privacy rights and will be the ones to bear the burden of this policy.

For the above reasons, it is likely that forensic searches of electronic devices at the border fall under the scope of the border exception. This means that there is no level of individualized suspicion required for the government to search a suspect at the border. This approach is consistent with the historical plenary power of the federal government at the border. Although these searches are not constitutionally prohibited, that does not mean that they are good policy. A policy like this has a high potential for abuse and thus should be curtailed. Therefore, a solution based in a source outside of the Fourth Amendment is likely required.

III. A LEGISLATIVE SOLUTION

Due to the fact that there is likely no constitutional protection against forensic searches of electronic devices at the border, congressional action is necessary. Absent

federal legislation, many of the previously discussed policy problems will continue to plague warrantless searches of electronic devices at the border. This part of the note will describe the elements of a potential legislative solution in order to address these concerns.

As was shown above, the approaches taken by each of the federal circuits come with policy defects. The approaches taken by the Fourth and Ninth Circuits require reasonable suspicion before an electronic device can be searched. Although this doctrine is at least partially restrictive, it is still too broad to meaningfully confine governmental actors. Additionally, it does not align with the historical arguments for the warrant exception. The constitutional arguments for the Eleventh Circuit's approach are sounder. However, the Eleventh Circuit's approach does not restrict forensic searches in any way and thus is ripe for abuse. Lastly, the First Circuit did not answer the question of whether reasonable suspicion is necessary for a forensic search and thus does not provide a solution. In fact, there is only one solution that will meaningfully confine government actors at the border and also satisfy constitutional requirements.

This solution is for Congress to pass a statutory requirement that would mandate a finding of probable cause before a suspect's electronic device can be searched at the border. This approach was alluded to by the Eleventh Circuit when it stated that there is nothing preventing "Congress from enacting laws that provide greater protections than the Fourth Amendment requires."[211] In doing this, Congress would address many of the policy concerns which arise under an arbitrary search

[211] United States v. Touset, 890 F.3d 1227, 1236 (11th Cir. 2018).

regime. This approach would also avoid the constitutional question entirely because a new statute would not have to be based in Fourth Amendment jurisprudence.

The proper standard for a statutory requirement would be probable cause because it is the standard that best preserves individual privacy rights as well as concepts of fairness within our criminal justice system. According to Professor Andrew Taslitz, the concept of privacy is fundamental to a free society.[212] This is because privacy is the metaphorical boundary that protects citizens "against the risk of being misdefined and judged out of context."[213] It is only in private that humans can be the truest versions of themselves and express themselves without fear of societal repudiation. Privacy is, therefore, necessary to preserve the autonomy of the individual in its truest form. For the state to intrude on something this fundamental, it should need a compelling justification.[214]

Under a reasonable suspicion approach or an approach that requires no individualized suspicion, the state does not need to produce any significant justification to intrude on this fundamental element of a free society. A probable cause requirement would mandate that officers have reasonably trustworthy information which is sufficient for "a man of reasonable caution" to believe that "an offense has been or is being committed."[215] This reasonable belief that an "offense has been committed" is sufficient to overcome the fundamental nature of privacy.[216] Without such a justification, the state is intruding on one of the most important societal

---

[212] Andrew E. Taslitz, *What is Probable Cause, and Why Should We Care?: The Costs, Benefits, and Meaning of Individualized Suspicion*, 73 DUKE L. & CONTEMP. PROBS. 145, 187 (2010).
[213] *Id.*
[214] *See id.* at 189.
[215] Brinegar v. United States, 338 U.S. 160, 175–76 (1949).
[216] *Id.*

mechanisms for preserving freedom and thus committing an unjust act.

Taslitz argues that the probable cause standard protects not just privacy rights, but also the basic fairness of our criminal justice system.[217] He states that there are two types of fairness concerns that probable cause addresses.[218] One is procedural fairness and the other is distributive fairness.[219] Procedural fairness encompasses the notion that every criminal defendant's case should be adjudicated according to the same set of rules.[220] If some searches can be conducted under probable cause and others under reasonable suspicion, we are acknowledging an unequal search process amongst criminal defendants. Professor Taslitz explains that an unequal standard gives the criminal suspect no control over whether he will be searched because the suspect will never know to which standard to hold himself.[221] Consequently, a reasonable actor would question whether his search was truly impartial and whether the officer's motives were transparent.[222] Therefore, by allowing this inequity to stand in our criminal justice system, we are allowing basic concepts of fair process to be violated because similarly situated individuals could be held to different standards.

Alternatively, distributive fairness requires that everyone should be charged the same "price" for safety.[223] As equal citizens bound in a social compact, we each agree to give the state certain search authority in order to preserve our safety. If we allow searches based on anything other than probable cause, some populations of society are paying an undue proportion of the price for safety. Those searched under a reasonable

---

[217] Taslitz, *supra* note 212, at 173–74.
[218] *Id.* at 174.
[219] *Id.*
[220] *Id.* at 175.
[221] *Id.* at 177.
[222] *Id.* at 177–79.
[223] *Id.* at 179.

suspicion standard have sacrificed more for the price of safety than those searched under probable cause. Therefore, the only equitable approach is to apply a uniform standard of probable cause.

For these reasons, probable cause is the best standard for any legislative solution. This standard best protects fundamental privacy rights as well as notions of fairness in our criminal justice system. This solution addresses the policy concerns that flow from the constitutional interpretations coming out of the United States circuit courts, without violating the Fourth Amendment. Consequently, a statutory probable cause requirement is the optimal solution.

Congress introduced legislation that included this statutory requirement in 2019 through the Protecting Data at the Border Act. [224] This act would have "prohibited the government from accessing the digital contents of an electronic device" without a warrant.[225] However, the bill never received a vote in the House of Representatives or the Senate. Additionally, this bill was an incomplete solution as the statutory protection was only extended to United States citizens and lawful permanent residents.[226] If Congress were to pass a probable cause requirement, it should be extended to all people. Otherwise, it would be completely permissible for federal agents to continue to arbitrarily search the cell phones of undocumented immigrants or law-abiding foreign travelers. Furthermore, federal agents have no meaningful way to distinguish United States citizens from other people, and invariably United States citizens will have their devices unjustly searched without this additional requirement.

[224] Protecting Data at the Border Act, S.823, 115th Congress, § 1 (2017).
[225] *Id.*
[226] *Id.*

Thus, until such legislation is passed, the electronic privacy rights of all persons within the United States' borders will continue to be threatened.

CONCLUSION

After analyzing the jurisprudence of the United States Circuit Courts of Appeals on the scope of the Fourth Amendment's border exception, this note revealed two dominant lines of analysis. The Fourth and Ninth Circuits hold that reasonable suspicion is required for the government to search a suspect's electronic device at the border. Although this approach was offered in good faith, the standard of reasonable suspicion does not meaningfully confine governmental actors and is constitutionally suspect. Conversely, the Eleventh Circuit holds that there is no level of individualized suspicion required for the government to conduct forensic searches of electronic devices at the border. This approach is consistent with the historical understanding of the border search exception. However, this approach has a high potential for abuse and could result in arbitrary searches being conducted. The First Circuit has now begun to weigh in on the subject but has yet to rule on the constitutionality of forensic searches.

This disagreement amongst the federal circuits presents an excellent opportunity for Congress to act. Congress has the authority to implement a new statutory probable cause requirement, without violating the original public meaning of the Fourth Amendment. This would address the negative policy concerns that come from each of the less restrictive standards while also maintaining our commitment to consistent Fourth Amendment jurisprudence.