"Please Unlock Your Phone": Why Reasonable Suspicion Should Be Extended to Cursory Searches of Electronic Devices at the Border

Will Carroll[1]

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[2]

I. Introduction

It is well established that the primary function of the Bill of Rights is to preserve essential liberties for citizens of the United States.[3] Cornerstone rights such as freedom of speech derive directly from the first ten amendments.[4] The protection of citizens from unreasonable searches and seizures by government agents also originates from the Bill of Rights.[5] The Fourth Amendment establishes:

> 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.[6]

As one scholar noted, the Fourth Amendment "makes plain, perhaps more than any other provision of the Bill of Rights, that the Constitution does not tolerate the tactics of a police state."[7] Unfortunately, U.S. border agents act with impunity, employing totalitarian, police state tactics by performing unconstitutional searches and seizures on a daily basis.[8] Although the right to be secure against unreasonable government intrusion is a vital freedom enjoyed by American citizens on the interior of the country, its sanctity is being violated at the border in an area dubbed the "Constitution-free zone."[9]

---

[1] J.D. Expected May 2019. Thank you to family, friends, and the Kentucky Law Journal staff for making this note possible.

[2] Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

[3] BILL OF RIGHTS INSTITUTE, BILL OF RIGHTS OF THE UNITED STATES OF AMERICA (1791), http://www.billofrightsinstitute.org/founding-documents/bill-of-rights/ (last visited Jan. 20, 2018).

[4] U.S. CONST. amend. I.

[5] Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 197 (1993).

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

[7] Maclin, *supra* note 5, at 197.

[8] *See CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. DEPARTMENT OF HOMELAND SECURITY, https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and (last modified Jan. 9, 2018).

[9] *See The Constitution in the 100-Mile Border Zone*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/other/constitution-100-mile-border-zone (last visited Jan. 22, 2018); *see also* Scott Bomboy, *Does a Constitution-Free Zone Really Exist in America?*, NATIONAL CONSTITUTION CENTER (Feb. 15, 2013), https://constitutioncenter.org/blog/does-a-constitution-free-zone-really-exist-in-america

Traditionally, border searches are exempt from Fourth Amendment protections in a doctrine known fittingly as the border search exception.[10] This exception exists "pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into [the U.S.]" and is "reasonable simply by virtue of the fact that [the searches] occur at the border."[11] In order to keep pace with rapidly advancing technology, some federal courts have explicitly extended the exception to electronic devices, holding that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."[12] This is particularly concerning because in today's world, smartphones, tablets, and laptops have rapidly shifted from a luxury to a daily necessity.[13] The Supreme Court recognized that "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[14]

The practice of searching electronic devices at the border has raised serious Constitutional concerns.[15] Statistics for the 2017 calendar year released by the U.S. Customs and Border Protection ("CBP") show that 30,200 international travelers, both inbound and outbound, were subjected to electronic device searches.[16] This is roughly a 37% increase from 2016.[17] CBP insists that "the need for border searches of electronic devices is driven by [their] mission to protect the American people and enforce the nation's laws in this digital age."[18] Many disagree with these border searches, and in September 2017, the American Civil Liberties Union ("ACLU") filed a lawsuit in federal court "on behalf of 11 travelers whose smartphones and laptops were searched without warrants at the U.S. border."[19] The ACLU's position is that Fourth Amendment protections should extend to border searches, "especially when it comes to electronic devices like smartphones and laptops."[20]

(explaining that the phrase "Constitution free zone" derives from the fact that border agents can search any electronic device without cause, thus bypassing traditional Fourth Amendment protections).

[10] *See* United States v. Ramsey, 431 U.S. 606, 620 (1977).

[11] *Id*. at 616.

[12] United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008). The standard of reasonable suspicion is defined as "a particularized and objective basis for suspecting the particular person stopped of criminal activity." United States v. Cortez, 4419 U.S. 411, 417-18 (1981). In making such a determination, "the totality of the circumstances—the whole picture—must be taken into account." *Id*. at 417.

[13] Emily Dreyfuss, *No, iPhones Aren't Luxury Items. They're Economic Necessities*, WIRED (Mar. 7, 2017), https://www.wired.com/2017/03/no-iphones-arent-luxury-items-theyre-economic-necessities/.

[14] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[15] Marcus Wolf, *Border Agents Can Legally Search Electronic Devices*, GOVERNMENT TECHNOLOGY (Apr. 17, 2017), http://www.govtech.com/security/Border-Agents-Can-Legally-Search-Electronic-Devices.html.

[16] U.S. Department of Homeland Security, *supra* note 8.

[17] *Id*. (19,051 in 2016 compared to 30,200 in 2017).

[18] *Id*.

[19] *Lawsuit on Behalf of 11 Travelers Challenges Searches of Electronic Devices as Unconstitutional*, AMERICAN CIVIL LIBERTIES UNION (Sept. 13, 2017), https://www.aclu.org/news/aclu-eff-sue-over-warrantless-phone-and-laptop-searches-us-border.

[20] Esha Bhandari, Nathan Freed Wessler, and Noa Yachot, *Can Border Agents Search Your Electronic Devices? It's Complicated*, AMERICAN CIVIL LIBERTIES UNION (Mar. 14, 2017), https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/can-border-agents-search-your-electronic.

The most recent development in border search exception precedent was decided by the Ninth Circuit in *United States v. Cotterman*.[21] In *Cotterman*, the court ruled that a forensic search of electronic devices at the border requires reasonable suspicion.[22] Forensic examination of computers is "a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites."[23] While this decision is certainly a step in the right direction, it fails to address the problem of unwarranted *cursory* searches of electronic devices. A cursory search, or "basic search" according to CBP, is any search that does *not* require "external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."[24] Cursory searches expose your electronic device's texts, emails, photos, internet history, and other personal information. This Note will argue that the reasonable suspicion standard currently applied to investigative searches of electronic devices at the border should be extended to cursory searches due to the clear violation of digital privacy and Fourth Amendment protections against unreasonable searches and seizures.

Part II of this Note will discuss basic Fourth Amendment principles and the origins of the border search exception with accompanying case law. Part III will unpack the Ninth Circuit's en banc decision in *United States v. Cotterman* and analyze the current situation of the border search exception. Part IV will illustrate arguments against extending reasonable suspicion to cursory searches of electronic devices at the border while presenting rebuttals to each of those arguments. Specifically, this Note argues that, in *United States v. Cotterman*, the Ninth Circuit should have extended the reasonable suspicion standard to cursory searches of electronic devices at the border. Part V lays out possible solutions to the issue and the impacts that might result from those solutions. Part VI concludes this Note.

II. A Brief Legal History of the Border Search Exception

The Fourth Amendment protects citizens against unreasonable searches and seizures unless the government has secured a warrant upon probable cause.[25] It is important to note that "the usual remedy for a Fourth Amendment violation is suppression of the illegally seized evidence"[26] via the exclusionary rule. The exclusionary rule is "a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation."[27] The key factor when applying the exclusionary rule is whether or not the individual had a reasonable

---

[21] United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).
[22] *Id*. at 957.
[23] *Id.*
[24] *CBP Directive No. 3340-049A: Border Search of Electronic Devices*, U.S. CUSTOMS AND BORDER PROTECTION (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.
[25] U.S. CONST. amend. IV.
[26] *Investigation and Police Practices*, 80 GEO. L.J. 939, 939 (1992).
[27] Davis v. United States, 564 U.S. 229, 231–232 (2011).

expectation of privacy in the area searched.[28] In his concurring opinion in *Katz v. United States*, Justice Harlan laid out the twofold test for determining whether an individual has an expectation of privacy in a certain area: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[29]

Exceptions to Fourth Amendment protections are common in the U.S. legal system such as the doctrines of plain view[30] and search incident to arrest.[31] These exceptions demonstrate the willingness of courts to mold the plain text of the Amendment to fit specific situations. For example, in *Carroll v. United States*, the Supreme Court ruled that warrantless searches of vehicles were permitted as long as the officer performing the search had probable cause.[32] The relevant language asserts that "[t]ravelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."[33] This language laid the initial groundwork for the border search doctrine and is often cited in cases utilizing the exception.[34]

Authority for the border search exception derives from several landmark Supreme Court decisions.[35] In justifying the border search doctrine, the Court has stated that the "exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."[36] In particular, "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[37] The Court has explicitly stated that "the expectation of privacy is less at the border than it is in the interior."[38] However, despite the broad language of border search exception cases, the Court has also implied that the Fourth Amendment might impose limits on border searches, but it has never definitively spoken on the subject.[39] Courts must balance "the sovereign's interests at the border" with the Fourth Amendment rights of the individual contesting the search.[40]

---

[28] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J. concurring).
[29] *Id*. at 361.
[30] *See* Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) ("It is well established that under certain circumstances the police may seize evidence in plain view without a warrant.").
[31] *See* Hill v. California, 401 U.S. 797, 804–805 (1971) (holding that a search incident to a valid arrest does not violate the Fourth Amendment).
[32] Carroll v. United States, 267 U.S. 132,154 (1925).
[33] *Id.*
[34] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 563 (1985) (Stevens, J. Concurring) (quoting *Carroll*, 267 U.S. at 154).
[35] *See* United States v. Ramsey, 431 U.S. 606 (1977); United States v. Flores-Montano, 541 U.S. 149 (2004).
[36] *Ramsey*, 431 U.S. at 620.
[37] *Flores-Montano*, 541 U.S. at 152.
[38] *Id*. at 154.
[39] United States v. Seljan, 547 F.3d 993, 999–1000 (9th Cir. 2008).
[40] United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985).

While the Supreme Court has addressed searches of persons[41] and vehicles[42] at the border, it has never directly ruled on the issue of searches of personal electronic devices at the border. The law on border searches of electronic devices derives mostly from the Courts of Appeals.[43] In *United States v. Arnold*, the Ninth Circuit extended the border search exception to electronic devices, holding that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."[44] Five years later, the Ninth Circuit was called on again to review the issue of border searches and electronic devices in *United States v. Cotterman*.[45]

III. *Cotterman* and Beyond

A. *United States v. Cotterman*

In *United States v. Cotterman*, Howard Cotterman and his wife were crossing the U.S.-Mexico border when he was flagged by the Treasury Enforcement Communication System for potentially possessing child pornography.[46] During the search of his vehicle, border agent Antonio Alvarado recovered and inspected three cameras and two laptops containing personal photos, along with several password-protected files.[47] The Cottermans were set free; however, suspecting that Mr. Cotterman had child pornography locked behind password-protection, the agents transported the laptops and cameras 170 miles to an off-site facility in order to conduct a forensic search of the devices.[48] The investigative search revealed hundreds of images of child pornography behind the password-protected files on Mr. Cotterman's laptop.[49]

After a grand jury indicted Mr. Cotterman for several offenses related to child pornography,[50] Mr. Cotterman moved to suppress the evidence claiming that it was acquired from an unlawful search and seizure violating his Fourth Amendment rights.[51] Following lower court proceedings, a divided three panel Ninth Circuit held that "reasonable suspicion was not required for the search and that 'the district court erred in suppressing the evidence lawfully obtained under border search authority.'"[52]

---

[41] *See id*. at 544.
[42] *See Flores-Montano*, 541 U.S. at 155-56.
[43] *See* United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).
[44] *Arnold*, 533 F.3d at 1008.
[45] United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).
[46] *Id*. at 957.
[47] *Id*. at 957-58.
[48] *Id*. at 958.
[49] *Id*. at 959.
[50] *Id*.
[51] *Id*.
[52] *Id*.

On rehearing en banc, the court ruled that forensic examination of electronic devices at the border requires a showing of reasonable suspicion.[53] The court explained that "[electronic devices] contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails,"[54] all of which "implicate[ ] the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.'"[55] In coming to their conclusion, the majority conceded that "legitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information."[56] The court stated that "[r]easonable suspicion is a modest, workable standard that is already applied in the extended border search, *Terry* stop, and other contexts."[57] Finally, the court reasoned that "[i]ts application to the forensic examination here will not impede law enforcement's ability to monitor and secure our borders or to conduct appropriate searches of electronic devices."[58]

The court applied this standard to Mr. Cotterman's case and ruled that the investigative search of his laptop was conducted upon reasonable suspicion and his "motion to suppress therefore was erroneously granted."[59] Although Mr. Cotterman was unable to suppress the evidence, the court correctly balanced "the sovereign's interests at the border" with the Fourth Amendment rights of the individual contesting the search.[60] Citing Justice Scalia, the court explained that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[61] However, the court did not completely overrule *Arnold*, which rejected the requirement of reasonable suspicion for both cursory and investigative searches of electronic devices.[62] In fact, they explicitly stated that "we have approved a quick look and uninstructive search of laptops."[63] While the court solved the issue of unreasonable investigative searches, the court is legitimizing the policy that cursory searches of personal electronic devices do not require reasonable suspicion.

---

[53] *Id*.at 968.
[54] *Id*. at 964.
[55] *Id*. (quoting U.S. CONST. amend. IV).
[56] *Id*. at 966.
[57] *Id*. In *Terry*, the Supreme Court explained that "[w]hen an officer is justified in believing that the individual whose suspicious behavior he is investigating at close range is armed and presently dangerous to the officer or to others, it would appear to be clearly unreasonable to deny the officer the power to take necessary measures to determine whether the person is in fact carrying a weapon and to neutralize the threat of a physical harm." Terry v. Ohio, 392 U.S. 1, 24 (1968). The Court ruled that "there must be a narrowly drawn authority to permit a reasonable search for weapons for the protection of the police officer, *where he has reason to believe* that he is dealing with an armed and dangerous individual, regardless of whether he has probable cause to arrest the individual for a crime." *Id*. at 27 (emphasis added). Reasonable suspicion generally requires that the officer "point[s] to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrants" an intrusion. *Id*. at 21.
[58] *Cotterman*, 709 F.3d at 966.
[59] *Id*. at 970.
[60] United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985).
[61] *Cotterman*, 709 F.3d at 965 (quoting Kyllo v. United States, 533 U.S. 27, 33–34 (2001)).
[62] United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008).
[63] *Id*. at 960.

B. The Current Situation

As a result of *Cotterman*, travelers can be confident that border agents lack the authority to perform investigative searches of their electronic devices without reasonable suspicion. This is clearly a win for digital privacy rights. Unfortunately, the problem of suspicionless cursory searches is still rampant, as demonstrated by the ACLU, which recently filed a lawsuit against the Department of Homeland Security challenging border searches of electronic devices.[64]

The concerning part of electronic device border searches stems from the fact that these are not isolated incidents. CBP released statistics for 2017 claiming that 30,200 international travelers, inbound and outbound, had their electronic devices searched.[65] That is roughly a 37% increase of electronic devices searched from 2016 to 2017.[66] CBP argues that national security outweighs the inconveniences of a small percentage of travelers, but privacy advocates disagree, stating that "[t]hey see the growth of a surveillance state eating away civil liberties a mouthful at a time."[67]

In early January 2018, CBP released a directive that outlined their procedures related to searching electronic devices at the border.[68] The directive states that "[t]he plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty."[69]

Outlining CBP procedures, the directive states:

> Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools or applications.[70]

Further, the directive distinguishes between basic and advanced border searches, articulating:

> In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border . . . An advanced search is any search in which an Officer connects external equipment, through a wired or wireless

---

[64] *See Lawsuit on behalf of 11 Travelers supra* note 19.
[65] U.S. Department of Homeland Security*, supra* note 8.
[66] *Id.*
[67] Frank Miniter, *Are You Okay With The Government Searching Your Cell Phone?*, FORBES (Jan. 8, 2018, 01:19PM), https://www.forbes.com/sites/frankminiter/2018/01/08/are-you-okay-with-the-government-searching-your-cell-phone/#173bca0410ed.
[68] U.S. Customs and Border Protection, *supra* note 25.
[69] *Id*.
[70] *Id.*

> connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.[71]

The directive requires CBP to obtain reasonable suspicion before performing an advanced search, i.e. an investigative search.[72] Here, it is clear they are abiding by *Cotterman*'s precedent. In *Cotterman*, the advanced search occurred when the password-protected files on Mr. Cotterman's computer were accessed by forensic software at the off-site facility.[73]

In sum, the 2018 CBP Directive continues to permit unconstitutional border searches.[74] In America, the people are taking a stand. For example, there has been a recent spike in publications instructing readers on how to protect their privacy at the border[75] and privacy complaints continue to be filed against the Department of Homeland Security.[76] Even with this resistance, these constitutional violations are unlikely to stop.[77] What is the next step?

The Supreme Court has never directly addressed border searches of electronic devices. In *Riley v. California* the Court ruled that "a warrant is generally required before [searching a cell phone], even when a cell phone is seized incident to arrest."[78] The Court recognized that because times have changed and modern smartphones contain highly private and sensitive data, the intrusion on privacy today is not limited to physical realities.[79] *Riley* proves that federal courts are at the very least cognizant of the importance of electronic devices and would be a logical place for the Supreme

---

[71] *Id*.
[72] *Id*.
[73] United States v. Cotterman, 709 F.3d 952, 958 (9th Cir. 2013).
[74] Sophia Cope & Aaron Mackey, *New CBP Border Device Search Policy Still Permits Unconstitutional Searches*, ELECTRONIC FRONTIER FOUNDATION (Jan. 8, 2018), https://www.eff.org/deeplinks/2018/01/new-cbp-border-device-search-policy-still-permits-unconstitutional-searches.
[75] *See* Hilary Beaumont, *Invasion of Privacy: Border Agents are Seizing Travellers' Phones and Asking for Their Passwords. Here's How to Protect Yourself*, VICE NEWS (Feb. 17, 2017), https://news.vice.com/en_ca/article/ywn8pj/how-to-secure-your-phone-when-crossing-the-border; Esha Bhandari, Nathan Freed Wessler, and Noa Yachot, *Can Border Agents Search Your Electronic Devices? It's Complicated*, AMERICAN CIVIL LIBERTIES UNION (Mar. 14, 2017), https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/can-border-agents-search-your-electronic; Rebecca Harrington, *Federal Agents Can Search Your Phone at the U.S. Border – Here's How to Protect Your Personal Information*, BUSINESS INSIDER (Sept. 13, 2017, 2:37 PM), http://www.businessinsider.com/can-us-border-agents-search-your-phone-at-the-airport-2017-2; and E.D Cauchi, *What if U.S. Border Agents Ask for Your Cellphone?*, NBC NEWS (Apr. 4, 2017), https://www.nbcnews.com/news/us-news/what-if-u-s-border-agents-ask-your-cellphone-n742511; Esha Bhandari, Nathan Freed Wessler, and Noa Yachot, *Can Border Agents Search Your Electronic Devices? It's Complicated*, AMERICAN CIVIL LIBERTIES UNION (Mar. 14, 2017), https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/can-border-agents-search-your-electronic.
[76] Charlie Savage, *Privacy Complaints Mount Over Phone Searches at US Border Since 2011*, BOSTON GLOBE, https://www.bostonglobe.com/news/nation/2017/12/23/privacy-complaints-mount-over-phone-searches-border-since/3Nk97AUtgK7wQEKZ0pkRnI/story.html.
[77] *Searches of Phones at the Border Unlikely to Stop*, Washington Examiner (Jan. 16, 2018, 12:01 AM), http://www.washingtonexaminer.com/searches-of-phones-at-the-border-unlikely-to-stop/article/2645452.
[78] Riley v. California, 134 S.Ct. 2473, 2493 (2014).
[79] *Id*. at 2489-90.

Court to start in making future rulings. Until then, however, it is important for lower courts to take the *Cotterman* decision one step further and apply the reasonable suspicion standard to cursory searches of electronic devices.

IV. Arguments Against Extending Reasonable Suspicion to Cursory Searches: the *Cotterman* Dissent

Judge Smith's dissenting opinion in *Cotterman* lays out three primary arguments against extending reasonable suspicion to cursory searches of electronic devices: administrative burdens, national security concerns, and the diminished expectation of privacy at the border.[80] Although Judge Smith's dissent was focused on the reasonable suspicion standard as applied to *investigative* searches of electronic devices, the same general arguments apply with equal force to *cursory* searches of electronic devices.

A. The Dangers of Administrative Burdens

The primary argument against extending reasonable suspicion to cursory searches of electronic devices at the border is that the additional step of requiring border agents to use their reasonable judgment will create a potentially dangerous administrative burden.[81] The dissent in *Cotterman* was concerned that "[r]equiring law enforcement to make such complex legal determinations on the spot, and in the face of potentially grave national security threats, strips agents of their necessary discretion and deprives them of an efficient and administrable rule."[82]

Border agents must rely on their broad discretion without case-by-case determination of individuals because "[they] process hundreds of thousands of travelers each day and conduct thousands of searches of electronic devices each year."[83] According to the dissent, forcing agents to comply with a case-by-case determination to conduct investigative searches of electronic devices at the border creates an undue burden due to the sheer number of individuals crossing the border every day.[84]

In practice, however, the reasonable suspicion standard would cause minimal administrative burdens on border agents while preserving the critical rights guaranteed by the Fourth Amendment. The *Cotterman* court best articulated the sentiment when it stated, "[r]easonable suspicion is a modest, workable standard that is already applied in the extended border search, *Terry* stop, and other contexts."[85] Continuing, the court explained that "[i]ts application to the forensic examination

---

[80] United States v. Cotterman, 709 F.3d 952, 981–94 (9th Cir. 2013) (Smith, J. dissenting).
[81] *Id*. at 982.
[82] *Id*.
[83] *Id*.
[84] *Id*.
[85] *Id*. at 966.

here will not impede law enforcement's ability to monitor and secure our borders or to conduct appropriate searches of electronic devices."[86]

The same can easily be said about cursory examination of electronic devices. The standard of reasonable suspicion is less than probable cause, requiring "merely 'a particularized and objective basis' for suspecting" the individual is engaging in criminal activity.[87] Simply requiring border agents to have some reasonable, objective basis for conducting a cursory search on a personal electronic device is hardly an administrative burden.

In the world of Constitutional Law, reasonable suspicion is a very moderate standard. The officer—or in cases of border searches, border agent—need not have a definitive certainty that the person is engaged in some unlawful conduct. Rather, the agent must assess the *totality of the circumstances*[88] and have some suspicion that the traveler coming through the border is involved in an illegal activity.

The dissent in *Cotterman* worries that the holding forces agents "to determine on a case–by–case and moment–by–moment basis whether a search of digital data remains 'unintrusive'…or has become 'comprehensive and intrusive.'"[89] A solution is to simply extend reasonable suspicion to cursory searches of electronic devices. The "complex legal determination[]"[90] the dissent seems to be worried about would not exist if border agents were not required to differentiate between investigative and cursory searches. Applying the reasonable suspicion standard to both types of searches clearly eliminates this problem.

B. The Interest in National Security

The *Cotterman* dissent also argued that there is an ever-present threat of terrorists entering the country.[91] Citing a U.S. Customs and Border Protection directive, Judge Smith explained that "border searches of electronic storage devices are 'essential' for 'detect[ing] evidence relating to terrorism and other national security measures.'"[92] Further, terrorists tend to rely on electronic storage devices for a multitude of uses such as copying and altering passports and other travel documents.[93] Therefore, "[b]y providing special privacy protections for electronic devices at the border, the majority eliminates the powerful deterrent of suspicionless searches and significantly aids" terrorists and criminals.[94] This sentiment has been

---

[86] *Id*.
[87] United States v. Tiong, 224 F.3d 1136, 1140 (9th Cir. 2000) (quoting Ornelas v. United States, 517 U.S. 690, 696 (1996)).
[88] The totality of the circumstances focuses on the entire situation rather than one specific factor. *Totality-of-the-Circumstances Test*, BLACK'S LAW DICTIONARY (10th ed. 2014).
[89] *Cotterman*, 709 F.3d at 984. When the dissent mentions an "unitrusive" search, they mean a cursory search, and a "comprehensive" search means an investigative search.
[90] *Id.* at 984.
[91] *Id*. at 984–85.
[92] *Id*. at 985 (U.S. Customs and Border Protection, *Border Search of Electronic Devices Containing Information*, CBP Directive No. 3340–049 § 1 (2009), https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf).
[93] *Cotterman*, 709 F.3d at 985.
[94] *Id*.

shared among scholars. One law review article suggests that the *Cotterman* decision has made it "more difficult for U.S. border agents to combat terrorism and child pornography" by carving "out a piece of the border search doctrine."[95]

Judge Smith predicted that "a reasonable suspicion requirement will likely disincentivize agents to conduct laptop searches in close cases."[96] Theoretically, border agents accused of conducting an unreasonable search will face "very real consequences" such as the possibility of being sued in their official capacities for civil damages.[97] By disincentivizing border agents from conducting searches of electronic devices for fear of reprimand or legal action against them, the dissent argues that "these misaligned incentives create unnecessary risk … for our entire nation."[98]

However, there is no proof that extending reasonable suspicion to cursory searches, let alone investigative searches, would negatively impact the efficiency of border agents in carrying out their duties. Requiring the agent to make a reasonable determination in light of the totality of the circumstances is not a significant burden on the agent's ability to carry out his duty. Reasonable suspicion "is a less demanding standard than probable cause and requires a showing *considerably less* than preponderance of the evidence."[99] The border agent simply needs to have "a minimal level of objective justification" for searching the phone.[100] This standard is extremely flexible and, at the very least, creates a baseline for Fourth Amendment protections of electronic devices at the border.

Further, the dissent's argument that attaching reasonable suspicion to a border search of an electronic device will somehow disincentivize border agents from conducting a search in the first place is unfounded. Simply because a border agent must use a minimal level of objective justification to search an electronic device does not mean they will be exposed to legal consequences. In fact, lawsuits have already been filed against CBP for the invasive searches conducted on electronic devices even without the reasonable suspicion standard.[101]

To assert that extending reasonable suspicion to searches of electronic devices would cause personal reprimand is baseless. If anything, it would diminish the number of lawsuits against CBP because the standard for conducting a search would be higher, theoretically resulting in a better-informed staff of border agents.

---

[95] Michael Creta, *A Step in the Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices During Border Searches in* United States v. Cotterman, B.C. L. REV E-SUPP., 2014, at 45. Michael Creta, *A Step in the Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices During Border Searches in United States v. Cotterman*, 55 B.C. L. REV E-SUPPLEMENT 31, 45 (2014).

[96] *Cotterman*, 709 F.3d at 985.

[97] *Id*.

[98] *Id*. at 986.

[99] Illinois v Wardlow, 528 U.S. 119, 123 (2000).

[100] *Id*.

[101] *See, e.g.,* Zack Huffman, *Homeland Security Sued Over Warrantless Tech Searches at Border*, COURTHOUSE NEWS SERVICE (Sept. 13, 2017), https://www.courthousenews.com/homeland-security-sued-warrantless-tech-searches-border/.

C. The Diminished Expectation of Privacy at the Border

Finally, the dissent in *Cotterman* suggests that searches of electronic data have never been immune to the border search exception.[102] Judge Smith questioned the privacy of electronic devices to begin with, explaining that electronic storage devices are "hardly a bastion of privacy" because "they transmit a massive amount of intimate data to the public on an almost constant basis."[103] According to Judge Smith, due to "the steady erosion of our privacy on the Internet, searches of electronic storage devices may be increasingly akin to a well-placed Internet search."[104] The dissent asserts that "[m]apping our privacy rights by the amount of information we carry with us leads to unreasonable and absurd results."[105]

The Supreme Court has explicitly stated that because "an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely."[106] Further, "not every search 'is acceptable solely because a person is in custody.'"[107] This same logic can be applied to travelers and border searches of electronic devices. The *Cotterman* court explained that "the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property."[108] There is no reason why this principle should not also apply to cursory searches as well. The Court has already implied that searching the cell phone of an arrestee without a warrant is an unreasonable intrusion into the arrestee's constitutional privacy due to the sensitive information contained on modern smartphones.[109] It is logical to apply the reasonable suspicion standard to cursory searches of electronic devices.

The Supreme Court explicitly stated that "the Fourth Amendment protects people, not places."[110] As the Court explained in *Riley*, "when 'privacy-related concerns are weighty enough' a 'search may require a warrant, notwithstanding the diminished expectations of privacy'" of the individual.[111] Even more so, this Note is *not* arguing that a warrant is required for a border search of an electronic device, rather it is arguing that the workable standard of reasonable suspicion be applied. As the Supreme Court noted in 1990:

> Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion

---

[102] *Cotterman*, 709 F.3d at 986.
[103] *Id*.
[104] *Id*.
[105] *Id*. at 987.
[106] Riley v. California, 134 S.Ct. 2473, 2488 (2014).
[107] *Id*. (quoting Maryland v. King, 569 U.S. 435, 463 (2013)).
[108] *Cotterman, 709 F.3d at 966 (majority opinion).*
[109] *Riley*, 134 S.Ct. at 2489–90.
[110] Katz v. United States, 389 U.S. 347, 351 (1967)
[111] *Riley*, 134 S.Ct. at 2488 (quoting Maryland v. King, 569 U.S. 435, 438 (2013)).

> can arise from information *that is less reliable than that required to show probable cause*.[112]

Pursuant to *Riley*, the privacy-related concerns in an individual's electronic device should clearly outweigh the diminished expectation of privacy at the border.

V. Solutions and Results

The most effective way to fix this problem is through legislative action. However, due in large part to partisan politics, the burden of responsibility for upholding U.S. citizens' Fourth Amendment rights in cases of electronic device border searches falls upon the federal courts. As discussed earlier, CBP's latest directive was clearly influenced by the *Cotterman* decision.[113] If courts take the initiative in restoring digital privacy rights by applying the reasonable suspicion standard to cursory searches of electronic devices, CBP would abide by that decision. Therefore, while legislative action would be the most effective and secure way to establish this standard, courts clearly have the ability to influence CBP policies.

What would the application of reasonable suspicion to cursory searches of electronic devices at the border entail? Although reasonable suspicion "is a less demanding standard than probable cause and requires a showing considerably less than preponderance of the evidence," there must still be some "minimal level of objective justification for making the stop."[114] In practice, a border agent would first need to assess the totality of the circumstances, i.e. the entire situation, as opposed to one specific factor.[115] Based on the totality of the circumstances, the agent would then make an objective determination as to whether the particular traveler was engaged in some type of criminal activity or may be a threat to national security.

For instance, if the agent observes physical manifestations of nervousness from a particular traveler such as profuse sweating or shaking, that might be enough to satisfy the reasonable suspicion standard. The Supreme Court has noted that "nervous, evasive behavior is a pertinent factor in determining reasonable suspicion."[116] Similarly, if the agent notices strange travel patterns in the traveler's documents, that too might be enough to meet the low standard of reasonable suspicion. Again, reasonable suspicion "does not deal with hard certainties, but with probabilities."[117] Applying this standard to cursory searches of electronic devices is a small demand, considering the privacy rights of U.S. citizens are being infringed upon by border agents on a daily basis.

VI. Conclusion

---

[112] Alabama v. White, 496 U.S. 325, 330 (1990) (emphasis added).
[113] *See* U.S. Customs and Border Protection, *supra* note 91.
[114] Illinois v. Wardlow, 528 U.S. 119, 123 (2000) (citing United States v. Sokolow, 490 U.S. 1, 7 (1989)).
[115] *Totality-of-the-Circumstances Test*, BLACK'S LAW DICTIONARY (10th ed. 2014).
[116] *Wardlow*, 528 U.S. at 124 (2000).
[117] United States v. Cortez, 449 U.S. 411, 418 (1981).

Courts need to extend reasonable suspicion to cursory searches of electronic devices at the border. Generally speaking, however, that would only be the start. The border search exception's detrimental effect on digital privacy is a stain on the integrity of the Constitution. The exception is a relic of the past in this age of rapid technological advancement. It clearly requires a new approach as we store more and more highly sensitive, confidential data on our phones, laptops, and tablets. At the end of the day, *Cotterman* was a strong starting point, but the next logical step is to extend the reasonable suspicion standard to cursory searches of electronic devices.