

CROSSING THE LINE: DEPARTMENT OF HOMELAND SECURITY BORDER
SEARCH OF MOBILE DEVICE DATA LIKELY UNCONSTITUTIONAL

ATANU DAS*

This Article discusses the constitutional limits regarding warrantless border searches of mobile device data by Custom and Border Patrol (CBP) officials. The Department of Homeland Security (DHS) has instituted rules to allow CBP officials to search the mobile device data of persons entering the United States without a warrant under the Border Search Exception doctrine of the Fourth Amendment. U.S. Supreme Court jurisprudence, however, has held that there are limits to warrantless border searches under the Border Search Exception doctrine without providing any further guidance. This Article provides analysis that the guidance for these limits can be found in established Fourth Amendment jurisprudence as well as recent U.S. Supreme Court case law, the results of which conclude that a border search of mobile device data likely requires obtaining a search warrant based on probable cause.

INTRODUCTION	206
I. WARRANTLESS SEARCH OF U.S. BORN CITIZENS' MOBILE DEVICE DATA BY AIRPORT BORDER SECURITY	211
II. U.S. SUPREME COURT JURISPRUDENCE HOLDS SOME BORDER SEARCHES MAY REQUIRE A WARRANT	212
A. From "Constitutionally Protected Places" to "Reasonable Expectation of Privacy"	213
B. Border Search Exception Doctrine Can Require a Warrant for Some Border Searches If "Particularly Offensive"	216
C. Lower Federal Court Rulings Are Likely Wrong Regarding Warrantless Border Search of Mobile Device Data	222
III. DHS RULES CALLING FOR WARRANTLESS SEARCH OF MOBILE DEVICE DATA ARE LIKELY UNCONSTITUTIONAL	228
IV. U.S. SUPREME COURT HOLDS SEARCH OF MOBILE DEVICE DATA NEEDS A WARRANT	229
V. ASCERTAINING THAT A PERSON HAS RIGHT TO ENTER THE UNITED STATES DOES NOT MEAN ASCERTAINING A PERSON IS NOT A TERRORIST	233
VI. SOME OF ACADEMIA RELUCTANT TO REQUIRE A WARRANT FOR A BORDER SEARCH OF MOBILE DEVICE DATA	235

* Distinguished Scholar in Residence, Loyola University Chicago, School of Law. The views in this Article are the author's own. A special thank you to Dean Michael Kaufman, Professor Barry Sullivan, Professor Spencer Waller, Professor Sacha Coupet, and Professor John Breen for their expertise, insight, and encouragement with regard to this Article. Also, I am grateful to my Research Assistant, Anne Bolamperti, who assisted me with editing, cite-checking, and researching for this Article. In addition, I would like to thank the wonderful editorial board and staff at the University of Pennsylvania Journal of Law and Social Change for their feedback, diligence, and effort to improve this Article to be the best it can be. Finally, my heartfelt thanks for the support and encouragement of my three sons, Roshan, Finn, and Leo, as well as the constant support and encouragement of my wife, Noreen, without which I would not be able to complete this work.

VII. CONCLUSION 238

INTRODUCTION

The Fourth Amendment protects U.S. citizens from unreasonable searches and seizures by government officials and law enforcement officers.¹ Barring an exception, the Fourth Amendment considers a reasonable search to be one conducted after law enforcement has obtained a search warrant from a judge based on probable cause.²

The U.S. Supreme Court jurisprudence regarding the Fourth Amendment finds several different exceptions in which a government official or law enforcement officer can conduct a reasonable search without first obtaining a warrant.³ These exceptions include a Search Incident to an Arrest,⁴ a Traffic Stop,⁵ and a Border Search.⁶ The Border Search Exception doctrine states that a government official or law enforcement officer can conduct a reasonable search without a warrant of a person and their belongings when entering the U.S. at the border.⁷ Department of Homeland Security (“DHS”) personnel, including Customs and Border Patrol (“CBP”) officials, as well as the

¹ U.S. CONST. amend. IV; *Katz v. United States*, 389 U.S. 347, 357 (1967) (stating “[s]earches conducted without warrants have been held unlawful ‘notwithstanding facts unquestionably showing probable cause,’ and . . . for the Constitution requires ‘that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police.’”) (quoting *Agnello v. United States*, 269 U.S. 20, 33 (1925) and *Wong Sun v. United States*, 371 U.S. 471, 481-82 (1963)).

² *Katz*, 389 U.S. at 357 (stating “searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.”).

³ *See, e.g., Carroll v. United States*, 267 U.S. 132, 153-154 (1925) (stating “[h]aving thus established that contraband goods concealed and illegally transported in an automobile or other vehicle may be searched for without a warrant, we come now to consider under what circumstances such search may be made . . . [T]he Fourth Amendment has been construed . . . as recognizing a necessary difference between a search of a . . . structure in respect of which a proper official warrant readily may be obtained, and a search of a [vehicle], for contraband goods, where it is not practicable to secure a warrant, because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought . . . Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in,” and thereby finding that the Border Search Exception doctrine is limited to warrantless border searches to determine whether a person can legally enter the United States or determine whether the person is bringing contraband, such as weapons or controlled substances into the United States.); *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (stating “explaining that Search Incident to an Arrest is a well-established exception for warrantless searches incident to the warrant requirement of the Fourth Amendment.”); *Delaware v. Prouse*, 440 U.S. 648, 663 (1979) (stating that it is constitutional under the Fourth Amendment for a vehicle to be stopped and searched without a warrant based on reasonable suspicion by law enforcement).

⁴ *Riley*, 134 S. Ct. at 2482.

⁵ *Prouse*, 440 U.S. at 663.

⁶ *Carroll*, 267 U.S. at 153-54.

⁷ *Id. See also* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 319 (2015) (stating “[u]nder the narrow approach, the border search exception exists to allow the government to keep out items that should be outside the United States . . . The underlying right is the right to control what enter . . . enters and exits the country.”).

courts, interpret this language broadly and possibly expand the limits of the Border Search Exception doctrine.⁸ As a result, the DHS has instituted rules⁹ and courts have issued decisions that give CBP officials almost unbridled authority to search a person and the person's belongings including mobile device data without a warrant at the U.S. border for any purpose.¹⁰

However, the DHS and the courts may have wrongly interpreted the Border Search Exception doctrine.¹¹ The U.S. Supreme Court held decades ago that the Border Search Exception doctrine has limits, albeit with no further guidance.¹² Nonetheless, Fourth Amendment

⁸ See, e.g., U.S. CUSTOMS AND BORDER PROTECTION, *Inspection of Electronic Devices*, (April 10, 2015), <https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf> (last visited March 1, 2018). [<https://perma.cc/E7RS-7XTF>]; WAYNE R. LAFAYE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, §10§ 10.5(a) (5th ed. 2017) (stating “[a]ny person or thing coming into the United States is subject to search by that fact alone, whether or not there be any suspicion of illegality directed to the particular person or thing to be searched.”) (citing *United States v. Odland*, 502 F.2d 148, 151 (7th Cir. 1974).

⁹ *Inspection of Electronic Devices*, See U.S. CUSTOMS AND BORDER PROTECTION, *supra* note 8.

¹⁰ See *United States v. Ickes*, 393 F.3d 501, 504-06 (4th Cir. 2005) (holding that there was statutory authorization to lawfully search the digital data content on Ickes’s computer and disks without a warrant based on reasonable suspicion because these constituted cargo as they were being transported in a vehicle crossing the border into the United States.); *United States v. Cotterman*, 709 F.3d 952, 970 (9th Cir. 2013) (holding that digital data content on Cotterman’s computer could be lawfully searched without a warrant based on reasonable suspicion.); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 570-571 (D. Md. 2014) (holding that the digital data content on Saboonchi’s computer could be lawfully searched without a warrant based on reasonable suspicion.). See also LAFAYE, *supra* note 8.

¹¹ *Inspection of Electronic Devices* See U.S. CUSTOMS AND BORDER PROTECTION, *supra* note 8. (stating “[a]ll persons, baggage, and merchandise [including mobile and electronic devices] arriving in, or departing from, the United States are subject to inspection, search and detention This is because CBP officers must determine the identity and citizenship of all persons seeking entry into the United States, determine the admissibility of foreign nationals, and deter the entry of possible terrorist, terrorist weapons, controlled substances, and a wide variety of other prohibited and restricted items.”). The Border Search Exception, however, does not give CBP officials unbridled authority to search electronic and mobile devices of a person without a warrant. Instead, the Border Search Exception allows for CBP officials to determine whether a person can legally enter the United States or conduct a search for contraband such as weapons or controlled substances. See *Carroll*, 267 U.S. at 153-154; *supra* note 8; *United States v. Ramsey*, 431 U.S. 606, 618, n.13 (1977) (stating “[w]e do not decide whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it is carried out,” thereby finding that there are some warrantless border searches that may be not be conducted lawfully but the Court does not provide any guidance in *Ramsey*). See *Katz*, 389 U.S. at 347, 361 (1967) (an example of Fourth Amendment jurisprudence by the Court providing guidance when a search (border search or otherwise) requires a warrant, and holding that “the rule that has emerged from prior decisions is that there is a twofold requirement, 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.’”). The Court has held that the amount of private information pertaining to a person stored on a mobile device itself and accessible on the Internet cloud from the mobile device is subject to a reasonable expectation of privacy such that the Search Incident to Arrest Exception to the warrant requirement does not apply, thereby requiring obtaining a warrant prior to searching the contents of a mobile device. See *Riley*, 134 S. Ct. at 2489-91 and 2494-95. The Court further held that “[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’” The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of protection for which the Founders fought. Our answer to the question of what police must do before search a cell phone seized incident to an arrest is accordingly simple – get a warrant.” *Id.* See *Carpenter v. United States*, 138 S. Ct. 2206, 2217, 2222 (2018) (holding that an individual has a legitimate expectation of privacy in their mobile device location information and due to this legitimate expectation of privacy a warrant is required prior to obtaining such mobile device location information.).

¹² *Ramsey*, 431 U.S. at 618 n. 13.

jurisprudence as well as recent U.S. Supreme Court case law has provided this long-sought guidance.¹³ This subsequent guidance indicates that CBP officials may be constitutionally required to obtain a warrant based on probable cause prior to conducting a border search of mobile device data.¹⁴

The Border Search Exception doctrine views the border or point of entry (i.e. airport, ship dock, etc.) to a country as a vulnerable place for both the sovereignty of the nation and the privacy interest of a person.¹⁵ Not only is the country vulnerable from people attempting to illegally enter the country or carry contraband, but also an individual's privacy interests are assailable as they may be violated for any number of significant or fickle reasons by border security officials.¹⁶ Thus, the Border Search Exception doctrine concedes that there are some border searches that may be "particularly offensive" to be unreasonable and possibly require a warrant.¹⁷ Court decisions dealing specifically with the Border Search Exception, however, do not provide any guidance on which border searches may require a warrant.¹⁸ This may be the reason the DHS and the courts have expanded the Border Search Exception doctrine to include warrantless border searches of a person and the person's belongings for any purpose.¹⁹ This expansive interpretation of the Border Search Exception doctrine includes searching mobile device data without a warrant at the border, even though the mobile device itself is found not to be contraband.²⁰ Further, the DHS seizes upon the

¹³ See *Katz*, 389 U.S. at 361; *Riley*, 134 S. Ct. at 2495.

¹⁴ *Inspection of Electronic Devices*, *supra* note 8, and accompanying text; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361; *Riley*, 134 S. Ct. at 2494-95.

¹⁵ See Thomas Mann Miller, *Digital Border Searches After Riley v. California*, 90 WASH. L. REV. 1943, 1996 (2015) (stating that an individual's privacy interest in their digital data content needs to be balanced with the traditional government interest of preventing people without a legal right to enter the U.S. from crossing the border and preventing contraband from entering the country.); See also Kerr, *supra* note 7, at 294-295 (stating "The Supreme Court has held that a border search exception to the Fourth Amendment applies to property entering and exiting the United States at the border, as well as its functional equivalent, in order to protect the sovereign interests of the United States in monitoring what enters and exits the country.").

¹⁶ *United States v. Montoya de Hernandez*, 473 U.S. 531, 552 (1985) (Brennan, J. dissenting and explaining "[the Fourth Amendment] is, or should be, an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly overzealous executive officers who are a part of any system of law enforcement.'" (citing *United States v. United States District Court*, 407 U.S., 297, 315 (1972)).

¹⁷ *Ramsey*, 431 U.S. at 618.

¹⁸ *Id.*

¹⁹ See Motion to Dismiss at 16-20, *Alasaad v. Duke*, No. 1:17-cv-11730 (D. Mass. Dec. 15, 2017); Kerr, *supra* note 7, at 319 (stating "Under the broad approach, the border search exception should allow the government to search everything entering and exiting the border to know what is entering and exiting the country.").

²⁰ *Ickes*, 393 F.3d at 505 (quoting *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004)) ("The reasonableness requirement is certainly met in this case, in light of the Supreme Court's recent instruction that searches of belongings at the border are 'reasonable simply by virtue of the fact that they occur at the border'"); *Cotterman*, 709 F.3d at 970 (holding that "the examination of Cotterman's electronic devices was supported by reasonable suspicion and that the scope and manner of the search were reasonable under the Fourth Amendment); *Saboonchi*, 990 F. Supp. 2d at 571 (holding that there was reasonable suspicion and thus that "officers did not violate the Fourth Amendment when they seized Saboonchi's Devices and subjected them to a forensic search"); see also Kerr, *supra* note 7, at 319 (stating "[b]ecause the [border search] exception allows for inspection of all physical items crossing the border, it should equally allow the inspection of all digital items crossing the border. The fact that so much more of the digital world crosses the border may expand government power, but it has no impact on the legal rule. The exception still applies . . .").

broad language of the Border Search Exception doctrine to search at the border not only data stored on the mobile device itself, but also email and social media content stored in the Internet cloud, which is accessible from the mobile device, which may be unconstitutional.²¹

Despite its broad language, the initial rationale of the Border Search Exception doctrine, the limits of a border search held by the U.S. Supreme Court, and overarching Fourth Amendment principles guide which border searches may be “particularly offensive” and points toward possibly requiring CBP to obtain a warrant based on probable cause.²² The initial rationale of the Border Search Exception doctrine justifies CBP officials conducting a warrantless search of a person and the person’s belongings only to ascertain whether the person can legally enter the U.S. and that they are carrying no contraband.²³ These should be construed to be the metes and bounds of the purpose for a warrantless border search.²⁴ Any further purpose for a border search should be viewed from the lens of Fourth Amendment jurisprudence, which states that a person has a reasonable expectation of privacy from a search conducted by law enforcement.²⁵ Thus, a person’s reasonable expectation of privacy in conjunction with the Border Search Exception doctrine should determine which border searches require a warrant.²⁶ Further, the DHS, lower federal courts, and even the U.S. Supreme Court, have found that a person has a reasonable expectation of privacy to shield their mobile device data from the peering eyes of the government.²⁷ Moreover, the U.S. Supreme Court has not once but twice indicated that mobile device data is so private that the Court provided it with special protections from law enforcement.²⁸ Therefore, I argue that the Border Search Exception doctrine’s initial rationale, its limits held by the U.S. Supreme Court, a person’s reasonable expectation of privacy, and recent U.S. Supreme Court holdings with regard to privacy protections of mobile device data should find a warrantless border search of mobile device data unreasonable, and thereby unconstitutional.²⁹

Within the past year, the U.S. government has made it clear that it wants a secure border.³⁰

²¹ *Inspection of Electronic Devices*, *supra* note 8. See Grinberg and Croft, *American NASA Scientist Says His Work Phone was Seized at Airport*, CNN, <https://www.cnn.com/2017/02/13/us/citizen-nasa-engineer-detained-at-border-trnd/index.html> (February 15, 2017, 5:57 PM) [<https://perma.cc/V6J2-2UFS>]. (“The Council on American Islamic-Relations reported increased scrutiny of American Muslims’ social media accounts and mobile phones while the [travel] ban was temporarily in effect.”) See Amended Complaint at 9, *Alasaad v. Duke*, No. 1:17-cv-11730 (D. Mass. Dec. 15, 2017) (“The number of border searches of electronic devices by CBP and ICE has been growing rapidly. According to CBP data, CBP conducted 14,993 electronic device searches in the first half of fiscal year 2017, meaning that CBP is on track to conduct approximately 30,000 searches this fiscal year, compared to just 8,503 searches in fiscal year 2015.”).

²² *Carroll*, 267 U.S. at 153-54; *Ramsey*, 431 U.S. at 618; *Katz*, 389 U.S. at 36 (Harlan, J., concurring).

²³ *Carroll*, 267 U.S. at 153-54; see also Miller, *supra* note 15.

²⁴ See *Ramsey*, 431 U.S. at 618 n. 13; see also Miller, *supra* note 15.

²⁵ *Katz*, 389 U.S. at 361.

²⁶ See *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361; *Riley*, 134 S.Ct. at 2494-95. See also Miller, *supra* note 15.

²⁷ *Cotterman*, 709 F.3d at 965-66.; *Riley*, 134 S. Ct. at 2478-79; *Carpenter*, 138 S. Ct. at 2217, See also LaFave, *supra* note 8 at §10.5(f) (stating “the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy.”) citing *Cotterman*, 709 F.3d at 966.”).

²⁸ Grinberg and Croft, *supra* note 21.

²⁹ *Carroll*, 267 U.S. at 153-54; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361. See also Miller, *supra* note 15.

³⁰ S.M., *Donald Trump’s Travel Ban Heads Back to the Supreme Court*, THE ECONOMIST—DEMOCRACY IN

A secure border has been framed by this administration as security from “illegal immigrants,” as individuals without documentation are often called, or security from “terrorists” that may want to do harm to people.³¹ A “terrorist” is defined by the FBI as a person with an ideology that includes committing violence against a country and/or its civilians for a political cause.³² A search of a person’s mobile device data, including email and social media content, can provide insight to CBP officials on whether the person has as considered by the government a “terrorist ideology.”³³ As part of a secure border, the U.S. government has made attempts to restrict people from entering the country through more stringent rules and regulations, as well as a more thorough vetting immigration process.³⁴ DHS rules seem to promote this policy by, arguably unconstitutionally, expanding the Border Search Exception doctrine beyond simply ascertaining whether a person can legally enter the U.S. and whether the person carries contraband.³⁵ The DHS rules use the fears about terrorism and security along with the Border Search Exception doctrine to justify expanding the scope of border searches.³⁶ The expansion of the search under the Border Exception Doctrine by the DHS rules to include the warrantless search of mobile device data likely makes such border searches unconstitutional.³⁷

This Article explains that the rationale of the Border Search Exception doctrine with its self-imposed limits coupled with a person’s reasonable expectation of privacy at the border under the *Katz* reasonable expectation of privacy test finds the warrantless border search of mobile device data as unreasonable and thereby likely unconstitutional in view of the Fourth Amendment.³⁸ Moreover, recent U.S. Supreme Court holdings further bolsters the assertion that a warrantless

AMERICA (Jan. 23, 2018), <https://www.economist.com/blogs/democracyinamerica/2018/01/travelling-ban> (last visited Feb 23, 2018) [<https://perma.cc/Y3VB-KK7K>].

³¹ Lawrence Hurley, *Supreme Court to Decide Legality of Trump Travel Ban*, REUTERS (Jan. 19, 2018, 2:12 PM), <https://www.reuters.com/article/us-usa-court-immigration/supreme-court-to-decide-legality-of-trump-travel-ban-idUSKBN1F82EY> [<https://perma.cc/63U9-CZUJ>] (stating that the travel ban was one way the U.S. government hoped to secure the border from terrorists masquerading as refugees to do harm against the U.S.).

³² See FBI, WHAT WE INVESTIGATE, <https://www.fbi.gov/investigate/terrorism> [<https://perma.cc/8642-YTQC>] (stating terrorism is conducted by people with extremist ideology); Roberto Iraola, *Terrorism, the Border, and the Fourth Amendment*, 2003 FED. CTS. L. REV. 1, *V.1 (2003) (stating “[t]he border exception to the Fourth Amendment provides the government with the necessary flexibility to detain and search persons and goods in its endeavor to protect the mainland and its citizens against acts of terrorism.”).

³³ *Inspection of Electronic Devices*, *supra* note 8. See Motion to Dismiss, *supra* note 19 at 3 (stating “Border searches of electronic devices are “a crucial tool for detecting information [relating] to terrorism.”) (quoting Border Search of Electronic Devices, ICE Directive No. 7 ¶ 4).

³⁴ *Trump’s executive order: Who does travel ban affect?* BBC NEWS (Feb. 10, 2017), <http://www.bbc.com/news/world-us-canada-38781302> [<https://perma.cc/49KN-HH23>].

³⁵ See Iraola, *supra* note 32. See also *Inspection of Electronic Devices*, *supra* note 8.

³⁶ See Iraola, *supra* note 32. See also *Inspection of Electronic Devices*, *supra* note 8.

³⁷ *Inspection of Electronic Devices*, *supra* note 8. See also Kerr, *supra* note 7.

³⁸ *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S. Ct. at 2494-95 (holding “[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans “the privacies of life. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.”). *Carpenter*, 138 S. Ct. at 2217, 2222 (holding that “an individual maintains a legitimate expectation of privacy” in mobile device location information and a warrant is required when a “suspect has a legitimate privacy interest in records help by a third party.”).

search of such mobile device data at the border is not reasonable and thereby is unconstitutional.³⁹

In addition, this Article discusses the likely unconstitutionality of warrantless border searches of mobile device data through the perspective of the real-life event of a U.S. citizen being detained under the DHS rules until he consented and provided the passcode of his mobile phone to CBP officials to allow them to search its data.⁴⁰ Through the backdrop of these events, the Article further explains the way in which the warrantless search of a U.S. citizen's mobile device data is likely unconstitutional under such circumstances.⁴¹ Finally, the Article synthesizes these ideas to show that the search of mobile device data at the border may require a warrant, in contrast to CBP officials' belief that warrantless border search of mobile device data is justified, and in contrast to some of academia's legal literature finding that only reasonable suspicion or probable cause may be necessary for such a search.⁴²

I. WARRANTLESS SEARCH OF U.S. BORN CITIZENS' MOBILE DEVICE DATA BY AIRPORT BORDER SECURITY

In January 2017, a U.S. born citizen, thirty-five-year-old Sidd Bikkannavar, was detained for a period of time at Houston's George Bush Intercontinental Airport while returning home from Chile.⁴³ While passing through customs and immigration procedures at the airport, CBP officials insisted on searching the data accessible from his mobile phone.⁴⁴ At first, he refused because he worked as a scientist for the National Aeronautics and Space Administration ("NASA")'s Jet Propulsion Laboratory ("JPL") in Pasadena, California,⁴⁵ and his mobile phone contained confidential information concerning his NASA work.⁴⁶ However, as CBP officials made it clear that his mobile phone could be seized indefinitely until he consented to the search, Bikkannavar relented and provided the passcode to his mobile phone to allow CBP officials to search its data.⁴⁷

Bikkannavar stated that CBP officials gave him a document titled "Inspection of Electronic Devices" indicating that the CBP had the right to search all people, baggage, and merchandise arriving in, or departing from, the United States.⁴⁸ Further, such a search was mandatory and the

³⁹ *Ramsey*, 431 U.S. at 618; *Riley*, 134 S. Ct. at 2494-95; *Carpenter*, 138 S. Ct. at 2217, 2222.

⁴⁰ Kavch Waddell, *A NASA Engineer Was Required to Unlock His Phone at the Border*, THE ATLANTIC (Feb. 13, 2017), <https://www.theatlantic.com/technology/archive/2017/02/anasaengineerisrequiredtounlockhisphoneattheborder/516489/> [<https://perma.cc/5CM5-WY6N>].

⁴¹ Amended Complaint, *supra* note 21 at 21-22; *Ramsey*, 431 U.S. at 618 n 13; *Katz*, 389 U.S. at 361; *Riley*, 134 S. Ct. at 2494-95; *Carpenter*, 138 S. Ct. at 2217, 2222.

⁴² Eunice Park, *The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post-Riley*, 44 HASTINGS CONST. L.Q. 277, 313-314 (2017) (stating "this Article urges that such a standard provides the balance that is needed between the critical interests of both law enforcement and the private individual."). See also Miller, *supra* note 15.

⁴³ Grinberg and Croft, *supra* note 21.

⁴⁴ Waddell, *supra* note 40.

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ Grinberg and Croft, *supra* note 21.

⁴⁸ Waddell, *supra* note 40. See also Amended Complaint, *supra* note 21. *Inspection of Electronic Devices* See U.S. CUSTOMS AND BORDER PROTECTION, *supra* note 8.

consequence for failure to cooperate could lead to the seizure of the mobile phone.⁴⁹ The rules indicated that one of the purposes of the warrantless border search of mobile device data included determining whether a person entering the U.S. had a terrorist ideology and to deter terrorists from entering the country.⁵⁰

Interestingly, Bikkannavar has been vetted by the government twice over to determine whether or not he was a national security risk.⁵¹ As a government scientist, he had gone through a thorough background check so that he could work with confidential information.⁵² Further, as part of the Customs and Border Protection Global Entry program that allows officials to waive him through customs lines after scanning his fingerprints, he had also submitted himself through another vetting process.⁵³ None of this mattered as CBP officials bullied him to provide them with the passcode to his mobile phone so that they could search its data without a warrant.⁵⁴

In September 2017, Bikkannavar and several co-plaintiffs, represented by the American Civil Liberties Union (“ACLU”), sued the DHS in Federal District Court in Massachusetts to find that the DHS rules allowing a warrantless border search of mobile device data are unconstitutional in view of the Fourth Amendment.⁵⁵ As discussed herein, the court should hold that they do so.

II. U.S. SUPREME COURT JURISPRUDENCE HOLDS SOME BORDER SEARCHES MAY REQUIRE A WARRANT

The Fourth Amendment holds that a person is free from unreasonable search and seizure by law enforcement officers.⁵⁶ The U.S. Supreme Court has evolved its Fourth Amendment jurisprudence over time such that law enforcement officers cannot search a person or the person’s belongings without a warrant issued by a judge based on probable cause.⁵⁷ However, the Court did hold that there are certain exceptional situations in which a warrantless search is reasonable which includes a warrantless search at the border.⁵⁸ As will be discussed herein, a warrantless border search to initially determine a person’s lawful entry and carrying of no contraband may be reasonable.⁵⁹ However, after such a determination, there may come a point during a warrantless border search becomes unreasonable or “particularly offensive” even under the Border Search

⁴⁹ Waddell, *supra* note 40.

⁵⁰ *Inspection of Electronic Devices See U.S. CUSTOMS AND BORDER PROTECTION*, *supra* note 8.

⁵¹ Waddell, *supra* note 40.

⁵² *Id.*

⁵³ *Id.*

⁵⁴ Amended Complaint, *supra* note 21.

⁵⁵ *Id.* at 39-40.

⁵⁶ U.S. CONST. Amend. IV.

⁵⁷ *Katz*, 389 U.S. at 353 (holding “[w]e conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the ‘trespass’ doctrine there enunciated can no longer be regarded as controlling.”) *See also Katz*, 389 U.S. at 361 (“[m]y understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, 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.’”) (Harlan, J., concurring).

⁵⁸ *Riley*, 134 S. Ct. at 2482; *Prouse*, 440 U.S. at 655-56 (1979); *Carroll*, 267 U.S. at 153-54.

⁵⁹ *Ramsey*, 431 U.S. at 618 n. 13; *Carroll*, 267 U.S. at 153-54. *See also Miller*, *supra* note 15 at 1954.

Exception doctrine.⁶⁰ Prior to discussing the Border Search Exception doctrine, it is imperative to understand the way in which the U.S. Supreme Court's jurisprudence on the Fourth Amendment has evolved.

A. From "Constitutionally Protected Places" to "Reasonable Expectation of Privacy"

Olmstead v. United States laid the groundwork for Fourth Amendment jurisprudence for decades.⁶¹ Its holding was overruled years later, but it is crucial to understand this case to provide the context of later Fourth Amendment jurisprudence.⁶²

In *Olmstead*, a U.S. Supreme Court case authored by former President and Chief Justice William Howard Taft, the Court dealt with wiretapping Roy Olmstead and his colleagues to determine whether they violated the Prohibition laws of the 1920s.⁶³ Prohibition officers wiretapped the telephone lines of Olmstead's offices in the basement of the office building as well as wiretapped his residential phone lines from the street.⁶⁴ Prohibition officers did not trespass either Olmstead's office or home to wiretap the phone lines.⁶⁵ The information gathered by Prohibition officers led to the conviction of Olmstead and his colleagues for violating Prohibition laws.⁶⁶

Chief Justice Taft's analysis of previous Fourth Amendment cases found that the Fourth Amendment protects "material things—the person, the house, his papers, or his effects" because the text of the Fourth Amendment itself states "the warrant . . . must specify the place to be searched and the person or things to be seized."⁶⁷ Further, Chief Justice Taft stated the invention of the telephone extended communications such that two people can talk to each other a great distance⁶⁸ but argued that the Fourth Amendment cannot be expanded to include telephone communications across such a great distance from the defendant's residence or place of business.⁶⁹ In addition, Chief Justice Taft analogized that the "intervening wires" of telephone communications are not part of Olmstead's residence or place of business, "any more than are the highways along which they are stretched."⁷⁰ Thus, Chief Justice Taft held "the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment."⁷¹

As a result of this ruling in 1928, the Fourth Amendment constitutionally protected a person's place such as his home or office as well as his tangible possessions, but not his ethereal voice conversations over telephone wires.⁷² Such a narrow interpretation of the Fourth Amendment would surprise modern day jurists, which find a more expansive protection of privacy interests

⁶⁰ *Ramsey*, 431 U.S. at 618 n. 13.

⁶¹ *Olmstead v. United States*, 277 U.S. 438, 468 (1928); *Katz*, 389 U.S. at 353.

⁶² *Olmstead*, 277 U.S. 438, 468 (1928).

⁶³ *Id.* at 456-57.

⁶⁴ *Id.* at 457.

⁶⁵ *Id.*

⁶⁶ *Id.* at 455-56.

⁶⁷ *Id.* at 464 (quoting U.S. CONST. Amend. IV.).

⁶⁸ *Id.* at 465.

⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ *Id.* at 466.

⁷² *Id.*

given by the Fourth Amendment.⁷³

As one may expect, *Olmstead*'s narrow holding was slowly expanded by subsequent U.S. Supreme Court cases.⁷⁴ Almost four decades after *Olmstead*, the U.S. Supreme Court remedied its narrow-minded decision.⁷⁵ In *Katz v. United States*, Charles Katz appealed from a conviction of violating wagering statutes when he collected wagering information over a telephone located in a phone booth in Los Angeles from Miami and Boston.⁷⁶ FBI agents placed electronic listening devices, without a search warrant, on the outside of the phone booth to record Katz's conversation.⁷⁷ Evidence from these recordings led to Katz's conviction.⁷⁸

Justice Stewart authored the majority opinion and found that "the underpinnings of *Olmstead* and *Goldman* have been so eroded . . . [in which] . . . the 'trespass' doctrine there enunciated can no longer be regarded as controlling."⁷⁹ Law enforcement officers that recorded Katz's voice conversations "violated the privacy upon which he justifiably relied while using the telephone booth and thus [their actions] constituted a 'search and seizure' within the meaning of the Fourth Amendment."⁸⁰ Further, Justice Stewart stated that "[t]he fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance," thereby ending the notion that the Fourth Amendment only "constitutionally protected places."⁸¹ Finally, Justice Stewart held that Fourth Amendment "considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth."⁸² Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.⁸³ The government agents here ignored the procedure of antecedent justification that is central to the Fourth Amendment, a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case.⁸⁴

⁷³ *Id.* at 361; *Katz*, 389 U.S. at 370 (*Katz* sets the stage for modern Fourth Amendment jurisprudence, finding that "[t]o support its new interpretation of the Fourth Amendment, which in effect amounts to a rewriting of the language of, the Court's opinion concludes that 'the underpinnings of *Olmstead* and *Goldman* have been eroded by our subsequent decisions.") (White, J., concurring). See also LAFAVE, *supra* note 8 at §2.1 (d) n. 127 (quoting John M. Junker, *The Structure of the Fourth Amendment Scope of the Protection*, 79 J. CRIM. L. & C. 1105, 1125-26 (1989)) (stating "What[w]hat is remarkable, however, is how little was changed by *Katz*'s abandonment of the 'trespass' standard of *Olmstead v. United States*.").

⁷⁴ *Katz*, 389 U.S. at 353. See LAFAVE, *supra* note 8 at § 2.1(b) (stating that subsequent Supreme Court cases since *Olmstead* eroded its holding thereby expanding Fourth Amendment protections).

⁷⁵ *Katz*, 389 U.S. at 370 (White, J., concurring); LAFAVE, *supra* note 8 at § 2.1 (d).

⁷⁶ *Katz*, 389 U.S. at 348.

⁷⁷ *Id.* at 348

⁷⁸ *Id.* at 348-49.

⁷⁹ *Id.* at 353.

⁸⁰ *Id.*

⁸¹ *Id.*; See also LAFAVE, *supra* note 8 at § 2.1 (b).

⁸² *Katz*, 389 U.S. at 359.

⁸³ *Id.*

⁸⁴ *Id.*; LAFAVE, *supra* note 8 at § 2.1(b) (stating "[t]he Court then proceeded to hold that the electronic eavesdropping, although apparently undertaken upon a 'strong probability' that Katz was using the telephone in violation of federal law, was an unconstitutional search because the agents had not first obtained a warrant.").

Katz is the basis of modern Fourth Amendment jurisprudence.⁸⁵ The *Katz* test that is used to analyze whether a search comports with the Fourth Amendment does not come from Justice Stewart's majority opinion but rather from Justice Harlan's concurring opinion.⁸⁶ Justice Harlan held that "[m]y understanding of the rule . . . is that there is a twofold requirement, 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.'" Justice Harlan further stated "[t]hus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."⁸⁷ On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.⁸⁸

Thus, *Katz* lays the foundation of modern Fourth Amendment jurisprudence.⁸⁹ Other than material possessions within the home hidden from plain view, a person has a privacy interest in other possessions, however, ethereal (e.g. voice conversations, electronic data, etc.) according to the *Katz* requirement of reasonable expectation of privacy.⁹⁰ Thus, if there is a privacy interest for a person's possession under the *Katz* requirement, then any reasonable search of that person's possessions by law enforcement requires a search warrant obtained based on probable cause.⁹¹

Although the Border Search Exception doctrine can be viewed as an exception to the warrant requirement in the Fourth Amendment, it still should work in conjunction with the *Katz* test.⁹² That is, the Border Search Exception doctrine balances the government's interest with a person's privacy interest.⁹³ Thus, for some types of searches at the border, a person would not have a reasonable expectation of privacy in view of the government's interest.⁹⁴ However, in other types of border searches, a person may have a reasonable expectation of privacy, that if carried out, would be "particularly offensive," unreasonable, and possibly require a warrant.⁹⁵

⁸⁵ *Kyllo v. United States*, 533 U.S. 27, 32-33 (2001).

⁸⁶ *Katz*, 389 U.S. at 348; *Kyllo*, 533 U.S. at 33.; LAFAVE, *supra* note 8 at § 2.1 (b) (stating "[i]n his concurring opinion in *Katz*, Justice Harlan indicated that he 'join[ed] the opinion of the Court,' but then explained what he took that opinion to mean. Because lower courts attempting to interpret and apply *Katz* quickly came to rely upon the Harlan elaboration, as ultimately did a majority of the Supreme Court . . .").

⁸⁷ *Katz*, 389 U.S. at 361.

⁸⁸ *Id.*; LAFAVE, *supra* note 8 at § 2.1(b).

⁸⁹ *Kyllo*, 533 U.S. at 32-33; *Riley*, 134 S. Ct. at 2497.

⁹⁰ *Katz*, 389 U.S. at 361; *Kyllo*, 533 U.S. at 32-33; *Riley*, 134 S. Ct. at 2497; LAFAVE, *supra* note 8 at § 2.1 (b).

⁹¹ *Katz*, 389 U.S. at 361.

⁹² *Ramsey*, 431 U.S. at 618; *Katz*, 389 U.S. at 361; LAFAVE, *supra* note 8 at § 2.1(b) (stating "It is important to realize that *Katz* did not merely extend Fourth Amendment protection to electronic surveillance. By redefining the basis upon which it could be said that a search and seizure had taken place, *Katz* also potentially altered all future applications of Fourth Amendments rights regarding searches and seizures.") citing Note, 23 CLEV. ST. L. REV. 63, 66 (1974). See also Kerr, *supra* note 7.

⁹³ Miller, *supra* note 15 at 1988.

⁹⁴ *Carroll*, 267 U.S. at 154. Park, *supra* note 42, at 282.

⁹⁵ See text *supra* note 11; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361; *Carpenter*, 138 S. Ct. at 2217.

B. Border Search Exception Doctrine Can Require a Warrant for Some Border Searches If “Particularly Offensive”

The Border Search Exception doctrine balances the sovereignty interest to protect the nation from unlawful entry of people and contraband with people’s reasonable expectation of privacy from searches of their person and belongings.⁹⁶ As indicated below, the Border Search Exception doctrine allows CBP officials to conduct a reasonable search without a warrant of a person and the person’s belongings at the border.⁹⁷ However, the genesis of the Border Search Exception doctrine was rooted in balancing sovereignty interests with the individual privacy interest, and this weighing of interests has been maintained as a backdrop in many cases invoking the Border Search Exception doctrine.⁹⁸

As modern Fourth Amendment jurisprudence evolved during the 20th century, so did the Border Exception to the Fourth Amendment.⁹⁹ The Border Search Exception doctrine was first promulgated in *Carroll v. United States*.¹⁰⁰ In that case, law enforcement officers stopped driver George Carroll and searched his automobile for contraband (i.e. liquor during the Prohibition) in Michigan, nowhere near a border.¹⁰¹

In *Carroll*, the law enforcement officer, two months prior to the stop, engaged in a sting operation to purchase illegal liquor from Carroll.¹⁰² At the time of the sting operation, the law enforcement officer noted that Carroll drove an Oldsmobile roadster automobile and mentioned that he needed to bring the liquor from a place east of Grand Rapids.¹⁰³ However, the sting operation was not successful, as Carroll never delivered the liquor.¹⁰⁴ Two months after the sting operation, the law enforcement officer patrolled a road east of Grand Rapids and recognized Carroll’s Oldsmobile Roadster.¹⁰⁵ Based on the evidence gathered from the sting operation, the law enforcement officer stopped and searched Carroll’s Oldsmobile roadster and found several dozen bottles of liquor.¹⁰⁶ The Court found evidence from the sting operation sufficient for probable cause to stop and search Carroll’s vehicle without a warrant.¹⁰⁷

Although the case was a vehicle stop within the borders of the country, which included a search of the automobile without a warrant, the Court stated that there are several exceptions to the

⁹⁶ *Katz*, 389 U.S. at 361; *Carroll*, 267 U.S. at 154; Miller, *supra* note 15 at 1988.

⁹⁷ See Iraola, *supra* note 32. Miller, *supra* note 15 at 1953-54.

⁹⁸ See *supra* note 11 and accompanying text; *Carroll*, 267 U.S. at 154.

⁹⁹ *Ramsey*, 431 U.S. at 618 n. 13; *United States v. Brignoni-Ponce*, 422 U.S. 873, 878 (1975); *Montoya de Hernandez*, 473 U.S. at 539-40.

¹⁰⁰ *Carroll*, 267 U.S. at 154; LAFAVE, *supra* note 8 at § 10.5(a) (stating that the United States Supreme Court did not have occasion to pass directly upon the question of whether routine searches of persons or things entering the country are permissible under the Fourth Amendment until *Carroll v. United States*).

¹⁰¹ *Carroll*, 267 U.S. at 160.

¹⁰² *Id.* at 134-35, 160.

¹⁰³ *Id.* at 135.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 135-36.

¹⁰⁷ *Id.* at 162.

Fourth Amendment requirement of obtaining a warrant from a judge based on probable cause.¹⁰⁸ Such exceptions include a vehicle stop and a border search.¹⁰⁹

Chief Justice Taft authored the opinion of the Court in *Carroll*¹¹⁰ and stated that the Fourth Amendment protects a person from *unreasonable* searches and seizures without a warrant.¹¹¹ It would be reasonable for a law enforcement officer to stop and search a vehicle without a warrant because a vehicle can move out of the jurisdiction before the law enforcement officer can obtain a warrant to stop and search the vehicle.¹¹² Thus, in *Carroll*, Chief Justice Taft held that the law enforcement officer can stop and search a suspect's vehicle without a warrant if the law enforcement office has probable cause to do so.¹¹³

Further, Chief Justice Taft explained a Border Search Exception to the Fourth Amendment as “[travelers] may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which maybe lawfully brought in.”¹¹⁴ Thus, the Border Search Exception was promulgated under the backdrop of a vehicle stop in which the Court was concerned that suspects may flee jurisdictions prior to law enforcement obtaining a search warrant.¹¹⁵ Moreover, the Court did state that “[t]he Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.”¹¹⁶ Therefore, the Border Search Exception was mired in the premise that it was in the public interest to ascertain a person's right to enter the U.S. and search to determine whether the person's possessions included contraband without a warrant because any suspect may flee the jurisdiction prior to obtaining a search warrant.¹¹⁷

In *United States v. Ramsey*, Justice Rehnquist further explained the Border Search Exception doctrine and its rationale and purpose.¹¹⁸ CBP officials invoked the Border Search Exception in this 1977 case to conduct a warrantless search of envelopes sent in the mail carrying narcotics.¹¹⁹ CBP officials found the envelopes were heavier than usual international mail and were from Thailand, a known source of narcotics.¹²⁰

Justice Rehnquist stated “[t]hat searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining people and their property crossing

¹⁰⁸ *Id.* at 153-54.

¹⁰⁹ *Id.*

¹¹⁰ *Carroll*, 267 U.S. at 136, 143.

¹¹¹ *Id.* at 147-49.

¹¹² *Id.* at 153-54.

¹¹³ *Id.* at 155-56; LAFAVE, *supra* note 8, at 221-22.

¹¹⁴ *Carroll*, 267 U.S. at 154; LAFAVE, *supra* note 8, at 222 (stating that border searches since the adoption of the Fourth Amendment have been considered “reasonable” by the fact that the person or item in question had entered into the country from outside.) (citing *United States v. Ramsey*, 431 U.S. 606, 619 (1977)).

¹¹⁵ *Carroll*, 267 U.S. at 153-54.

¹¹⁶ *Id.* at 149.

¹¹⁷ *Id.* 153-154.

¹¹⁸ *Id.* at 617-18.

¹¹⁹ *Id.* at 609-10.

¹²⁰ *Id.* at 609.

into this country, are reasonable simply by virtue of the fact that they occur at the border.¹²¹ Justice Rehnquist went on to cite *Carroll* by quoting “[i]t would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search.¹²²” In addition, Justice Rehnquist reiterated that the Border Search exception from *Carroll* provides for a warrantless search of a person and the person’s belongings to ascertain whether the person can legally enter the United States and whether the person is carrying contraband.¹²³ Finally, Justice Rehnquist held that “[b]order searches, then, from before the adoption of the Fourth Amendment, have been considered to be ‘reasonable’ by the single fact that the person or item in question had entered into the country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause.”¹²⁴ Justice Rehnquist further stated that such warrantless border searches were “‘reasonable’” and “[have] a history as old as the Fourth Amendment itself.”¹²⁵

However, buried in a footnote, Justice Rehnquist stated “[w]e do not decide whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it is carried out.”¹²⁶ In this footnote, Justice Rehnquist acknowledged limits to warrantless border searches under the Border Search Exception doctrine,¹²⁷ but provided no guidance to the extent of the limits.

Stepping back from Border Search Exception doctrine jurisprudence and viewing the overarching Fourth Amendment principles may provide the answer to the limits of the Border Search Exception doctrine.¹²⁸ *Ramsey* was decided ten years after *Katz* and fifty years after *Carroll*.¹²⁹ The limits of the Border Search Exception doctrine should be determined in conjunction with its initial rationale from *Carroll* and a person’s reasonable expectation of privacy from the *Katz* test.¹³⁰ Thus, the confluence of *Carroll*, *Katz*, and *Ramsey*, results in a person having no reasonable expectation of privacy from certain types of border searches in a narrow circumstance - those that ascertain that the person has a legal right to enter the U.S. and carries no contraband.¹³¹ However, the Supreme Court jurisprudence resulting from the combination of *Carroll*, *Katz*, and *Ramsey* also holds that a person may have a reasonable expectation of privacy with regard to other

¹²¹ *Id.* at 616.

¹²² *Id.* at 618.

¹²³ *Id.*

¹²⁴ *Id.* at 619; LAFAVE, *supra* note 8, at 223 (stating “[t]he lower courts have consistently held, both before and after *Ramsey*, that routine searches of persons and things may be made upon their entry into the country.”).

¹²⁵ *Ramsey*, 431 U.S. at 619.

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ See *supra* note 11. and accompanying text; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S.; *Katz*, 389 U.S. at 361.

¹²⁹ *Carroll*, 267 U.S. at 132; *Ramsey*, 431 U.S. at 606. ; *Katz*, 389 U.S. at 347.

¹³⁰ *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13.; *Katz*, 389 U.S. at 361. See also Miller, *supra* note 15.

¹³¹ *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 518. *Katz*, 389 U.S. at 361. See Miller, *supra* note 15, at 1953-54.

types of border searches beyond this narrow circumstance.¹³² Thus, these types of border searches may be “particularly offensive” and unreasonable, and thereby likely unconstitutional if conducted without a warrant.¹³³

One invasive case of search and seizure of persons under the Border Search Exception doctrine was *United States v. Montoya de Hernandez*.¹³⁴ At first glance, this case may indicate an expansion of the Border Search Exception doctrine,¹³⁵ but after further consideration, it reveals that the conducted search is within the traditional limits of the Border Search Exception doctrine.¹³⁶ In this 1985 case, CBP officials at Los Angeles International Airport suspected Montoya de Hernandez of smuggling drugs in her alimentary canal based on her frequent trips between Bogotá, Colombia, and Los Angeles, California.¹³⁷ CBP officials searched her and determined that she was wearing a girdle and elastic underpants lined with paper towels, indicating she was smuggling drugs in her alimentary canal.¹³⁸ As a result, CBP officials detained Montoya de Hernandez for sixteen hours, during which time CBP officials obtained a warrant from a Federal Magistrate to conduct a rectal search.¹³⁹ After conducting this search, it was found that Montoya de Hernandez was indeed smuggling drugs in her alimentary canal.¹⁴⁰

Justice Rehnquist stated that the Border Search Exception doctrine “[b]alanced against the sovereign’s interests at the border [and] the Fourth Amendment rights of respondent.”¹⁴¹ Further, Justice Rehnquist found,

respondent was entitled to be free from unreasonable search and seizure. But not only is the expectation of privacy less at the border than in the interior, the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border.¹⁴²

Finally, Justice Rehnquist held “that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is

¹³² *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13. *Katz*, 389 U.S. at 361. See Miller, *supra* note 15, at 1953-54. But see LAFAVE, *supra* note 8 at §10.5(f) at 260–65 (outlining the line of Supreme Court cases that all but eliminate the reasonable suspicion requirement before a warrantless search).

¹³³ See *supra* note 11 and accompanying text; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618; *Katz*, 389 U.S. at 361; Kerr, *supra* note 7.

¹³⁴ *Montoya de Hernandez*, 473 U.S. at 541.

¹³⁵ *Id.* at 539.

¹³⁶ *Id.* at 540-41. See Miller, *supra* note 14, at 1953-54 (stating that the historical justification of the Border Search Exception doctrine is to determine whether a person can legally enter the United States or whether a person’s belongings include contraband).

¹³⁷ *Montoya de Hernandez*, 473 U.S. at 533; LAFAVE, *supra* note 8 at §10.5(b) at 233.

¹³⁸ *Montoya de Hernandez*, 473 U.S. at 534.

¹³⁹ *Id.* at 535-536.

¹⁴⁰ *Id.* at 535–36; LAFAVE, *supra* note 8 at §10.5(b) at 233.

¹⁴¹ *Montoya de Hernandez*, 473 U.S. at 539.

¹⁴² *Id.* at 539-40.

smuggling contraband in her alimentary canal.”¹⁴³

Although one view of this case may be that it expanded the Border Search Exception doctrine to allow for the invasive, warrantless search of a person’s alimentary canal,¹⁴⁴ in actuality the search was conducted within the limits of the Border Search Exception doctrine that include ascertaining whether a person is carrying contraband into the U.S.¹⁴⁵ Specifically, the border search was to determine whether Montoya de Hernandez was smuggling contraband in her alimentary canal.¹⁴⁶ However, Rehnquist found that such a search of the alimentary canal must be conducted only if there is reasonable suspicion of contraband being smuggled.¹⁴⁷ Thus, the unbridled authority to search a person for carrying contraband without any reasonable suspicion had been reined in by the Court with *Montoya de Hernandez*.¹⁴⁸ That is, prior to this case, it was unclear whether CBP officials could search a person and the person’s belongings for contraband without any need for reasonable suspicion.¹⁴⁹ However, in *Montoya de Hernandez*, Rehnquist said that, for invasive body searches, reasonable suspicion is needed, thereby limiting the Border Search Exception doctrine.¹⁵⁰ Further, *Montoya de Hernandez* does not deviate from the limit of the Border Search Exception doctrine stated in *Ramsey* and found in *Carroll*, which held that any further search beyond ascertaining whether a person has a legal right to enter the U.S. and is carrying no contraband may require a search warrant if it were “particularly offensive” and unreasonable.¹⁵¹

Moreover, Justice Brennan, in his dissent, lambasted Justice Rehnquist, stating search and seizures conducted by CBP officials on Montoya de Hernandez are that of a police state and not of free society as this country.¹⁵² Justice Brennan advocated limiting the Border Search Exception doctrine even further than Justice Rehnquist by stating that such an intrusive search cannot be based simply on reasonable suspicion, but rather can only be based on probable cause and approval of a judicial officer.¹⁵³ Such a holding would still balance the country’s public interest with the individual’s privacy interest as iterated by Justice Rehnquist.¹⁵⁴ If left unchecked, Justice Brennan feared that overzealous officers may run afoul of the Fourth Amendment and illegally search and seize people at the border.¹⁵⁵

¹⁴³ *Id.* at 549-50; LAFAVE, *supra* note 8 at §10.5(b.) at 234.

¹⁴⁴ *Montoya de Hernandez*, 473 U.S. at 541 (holding “that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal.”).

¹⁴⁵ *Id.* at 541-42 (holding “[u]nder this standard officials at the border must have a ‘particularized and objective basis for suspecting the particular person’ of alimentary[] canal smuggling.”).

¹⁴⁶ *Id.* at 542.

¹⁴⁷ *Id.*

¹⁴⁸ *Id.*; LAFAVE, *supra* note 8 at §10.5(b.) at 233-34.

¹⁴⁹ *Montoya de Hernandez*, 473 U.S. at 541.

¹⁵⁰ *Id.*

¹⁵¹ *Ramsey*, 431 U.S. at 617-18; *Montoya de Hernandez*, 473 U.S. at 541. *See also* Miller, *supra* note 15, at 1953-54.

¹⁵² *Montoya de Hernandez*, 473 U.S. at 546-50.

¹⁵³ *Id.* at 552; LAFAVE, *supra* note 8 at §10.5(b) at 237 (stating that the silence of the majority on whether such a search in *Montoya de Hernandez* requires a warrant is particularly significant).

¹⁵⁴ *Montoya de Hernandez*, 473 U.S. at 541.

¹⁵⁵ *Id.* at 565-67.

One could argue that Justice Brennan's analysis of the facts in *Montoya de Hernandez* through the lens of *Carroll*, *Ramsey*, and *Katz*.¹⁵⁶ That is, *Carroll* provided the genesis of the Border Search Exception doctrine allowing a warrantless search of a person to ascertain whether the person can legally enter the U.S. and ascertain whether the person's belongings have any contraband,¹⁵⁷ *Ramsey* found that there can be searches at the border, which can be particularly offensive, that could possibly require a search warrant,¹⁵⁸ and *Katz* provided the guidance on which border searches are particularly offensive.¹⁵⁹ Justice Brennan found that a person has a reasonable expectation of privacy of her alimentary canal from a warrantless search at the border, even if it is to ascertain whether the person is smuggling contraband into the United States. Thus, his insistence that such a border search be conducted after obtaining a warrant is based on probable cause.¹⁶⁰

Another invasive search of a person's belongings conducted under the Border Search Exception was in *United States v. Flores-Montano*.¹⁶¹ In this 2004 case, a vehicle crossing the border was stopped by CBP officials and asked to proceed to a secondary inspection area without any reasonable suspicion.¹⁶² At the secondary inspection area, another CBP official tapped the vehicle's gas tank and found that it sounded solid as opposed to hollow.¹⁶³ With this further suspicion, a mechanic was ordered to disassemble the gas tank, which revealed that the driver was smuggling drugs in the gas tank.¹⁶⁴

Chief Justice Rehnquist stated that the "[g]overnment's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."¹⁶⁵ Further, Chief Justice Rehnquist found "[t]ime and again, we have stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'"¹⁶⁶ Finally, Chief Justice Rehnquist held that the "[g]overnment's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank."¹⁶⁷ However, Chief Justice tempered this holding by stating that

¹⁵⁶ *Id.* at 551, 553–54.

¹⁵⁷ *See Carroll*, 267 U.S. at 154; Miller, *supra* note 15, at 1953-54.

¹⁵⁸ *See Ramsey*, 431 U.S. at 606.

¹⁵⁹ *See Katz*, 389 U.S. at 361; *see also Montoya de Hernandez*, 473 U.S. at 559-60.

¹⁶⁰ *Carroll*, 267 U.S. at 154. *Ramsey*, 431 U.S. at n. 13. *Katz*, 389 U.S. at 361. *See also Montoya de Hernandez*, 473 U.S. at 555 (holding that "[e]ven assuming that border detentions and searches that become lengthy and highly intrusive need not be supported by probable cause, but see Part II, *infra*, this reasoning runs squarely contrary to the Court's administrative-warrant cases. We have repeatedly held that the Fourth Amendment's purpose of safeguarding 'the privacy and security of individuals against arbitrary invasions by government officials' is so fundamental as to require, except in 'certain carefully defined classes of cases,' a magistrate's prior authorization even where '[p]robable cause in the criminal law sense is not required.") (internal citations omitted).

¹⁶¹ *United States v. Flores-Montano*, 541 U.S. 149, 151 (2004).

¹⁶² *Flores-Montano*, 541 U.S. at 155-56.

¹⁶³ *Id.* at 151.

¹⁶⁴ *Id.*

¹⁶⁵ *Id.* at 152.

¹⁶⁶ *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

¹⁶⁷ *Id.* at 155. *See also LAFAVE*, *supra* note 8 at §10.5(f) at 261-62 ("[T]he reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person has no expectation of -dignity and privacy at the border from interests of the person being searched-simply do not carry over to vehicles. Complex balancing

“[w]hile it may be true that some searches of property are so destructive as to require a different result, this was not one of them.”¹⁶⁸ *Flores-Montano* did not expand the Border Search Exception doctrine beyond ascertaining whether a person can legally enter the U.S. or whether the person is carrying contraband.¹⁶⁹ A person does not have a reasonable expectation of privacy from a warrantless search of his or her vehicle’s gas tank for contraband at the border.¹⁷⁰ However, Chief Justice Rehnquist’s tempered holding can lead to the conclusion that the Court may find that further searches of a person’s belongings at the border could require reasonable suspicion, probable cause, or even require a warrant if a person has a reasonable expectation of privacy to such belongings.¹⁷¹

C. Lower Federal Court Rulings Are Likely Wrong Regarding Warrantless Border Search of Mobile Device Data

Although there is no U.S. Supreme Court case that deals with searching mobile device data at the border, lower courts have dealt with the issue.¹⁷² One such case is *United States v. Ickes* from the Fourth Circuit.¹⁷³ In this 2004 case, John Ickes was driving from Canada into the United States near Detroit, Michigan.¹⁷⁴ At the border entry point, Ickes told a CBP official that he was returning to the United States from vacation.¹⁷⁵ The CBP official found this suspicious because a cursory inspection of Ickes’ vehicle indicated that it carried many of his belongings, so much so that it looked as if it stored everything he owned.¹⁷⁶ Consequently, the CBP official directed Ickes to a secondary inspection area where another CBP official conducted a more thorough secondary search.¹⁷⁷ Initially, the secondary search revealed a video camera containing a tape of a tennis match that suspiciously focused on a ball boy.¹⁷⁸ Further into the search revealed that Ickes’ vehicle contained marijuana paraphernalia, a copy of an arrest warrant from Virginia, and a photo album of child pornography.¹⁷⁹ At this point, the CBP officials arrested Ickes, ran his personal information,

tests to determine what is a ‘routine’ search of the passenger compartment of a vehicle. Further, as opposed to a gas tank’s sole purpose is to store fuel. Therefore, a person has a less expectation of privacy in a border more ‘intrusive’ search of the vehicle’s gas tank than a person, have no place in a border search of the passenger compartment vehicles.”) (quoting *Flores-Montano*, 541 U.S. at 152).

¹⁶⁸ *Flores-Montano*, 541 U.S. at 155-56.

¹⁶⁹ *Id.* at 154; Miller, *supra* note 15, at 1953-54.

¹⁷⁰ *Flores-Montano*, 541 U.S. at 152-53.

¹⁷¹ See, e.g., *Flores-Montano*, 541 U.S. at 155-56 (“While it may be true that some searches of property are so destructive as to require a different result, this was not one of them.”); *Ramsey*, 431 U.S. at 618 n.13 (“We do not decide whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it is carried out.”).

¹⁷² *Ickes*, 393 F.3d at 502; *Cotterman*, 709 F.3d at 952; *Saboonchi*, 990 F. Supp. 2d at 536.

¹⁷³ *Ickes*, 393 F.3d at 501.

¹⁷⁴ *Id.* Kerr, *supra* note 7 at 295.

¹⁷⁵ *Ickes*, 393 F.3d at 501.

¹⁷⁶ *Id.*

¹⁷⁷ *Id.*

¹⁷⁸ *Id.*

¹⁷⁹ *Id.* at 502-03.

and found that he had two outstanding arrest warrants against him.¹⁸⁰ Additional search of the vehicle revealed more child pornography stored on his computer.¹⁸¹

Ickes appealed the denial of his motion to suppress the evidence found on his computer, arguing that the search was unconstitutional.¹⁸² Judge Wilkinson cited *Ramsey*, *Montoya de Hernandez*, and *Flores-Montano* to find that the Border Search Exception doctrine gave CBP officials authority to search the contents of a computer for contraband such as child pornography.¹⁸³ However, Judge Wilkinson implied that particularized suspicion from a cursory and secondary inspection of Ickes' vehicle led to a more intrusive search of the Ickes' mobile device data.¹⁸⁴ Thus, Judge Wilkinson seemed to intimate that some sort of reasonable suspicion is needed to conduct a border search of mobile device data.

Judge Wilkinson's instincts comported with the rationale underlying the Border Search Exception.¹⁸⁵ However, his instincts did not go far enough.¹⁸⁶ That is, the Border Search Exception doctrine states that warrantless search is only reasonable to determine whether a person can legally enter the U.S. and whether the person's belongings contain contraband.¹⁸⁷ Any further search may violate a person's reasonable expectation of privacy and may require a warrant based on probable cause because such search may be "particularly offensive."¹⁸⁸

Thus, Judge Wilkinson found that a more particularized suspicion was needed to justify the border search of the mobile device data.¹⁸⁹ Such a finding is synchronous with the rationale that once a person is determined to have a legal right to enter the U.S. and is carrying no contraband, then the person's privacy interests are heightened.¹⁹⁰ That is, once it is determined that Ickes' mobile devices themselves were not contraband (e.g. weapons), then Ickes' privacy interest in any further search of the mobile devices is heightened.¹⁹¹ Therefore, Judge Wilkinson justified the further

¹⁸⁰ *Id.*

¹⁸¹ *Id.* at 503.

¹⁸² *Id.*

¹⁸³ *Id.* at 504-05. *See also* Kerr, *supra* note 7 at 295.

¹⁸⁴ *See Ickes*, 393 F.3d at 502.

¹⁸⁵ *Id.* at 506 ("The essence of border search doctrine is a reliance upon the trained observations and judgments of customs officials, rather than upon constitutional requirements applied to the inapposite context of this sort of search.").

¹⁸⁶ *See Ramsey*, 431 U.S. at 618 n. 13.

¹⁸⁷ *Id.* *See Carroll*, 267 U.S. at 154 ("Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in. But those lawfully within the country, entitled to use the public highways, have a right to free passage without interruption or search unless there is known to a competent official, authorized to search, probable cause for believing that their vehicles are carrying contraband or illegal merchandise."). *See also* Miller, *supra* note 15, at 1953-54.

¹⁸⁸ *Ramsey*, 431 U.S. at 618 n. 13. *See also Carroll*, 267 U.S. at 155-56 ("The measure of legality of such a seizure is, therefore, that the seizing officer shall have reasonable or probable cause for believing that the automobile [sic] which he stops and seizes has contraband liquor therein which is being illegally transported. . . . In cases where seizure is impossible except without warrant, the seizing officer acts unlawfully and at his peril unless he can show the court probable cause.").

¹⁸⁹ *Ickes*, 393 F.3d at 507.

¹⁹⁰ *See supra* note 11. *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Carpenter*, 138 S. Ct. at 2217.

¹⁹¹ *See supra* note 11. *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361;

search of the mobile device data based on the particularized suspicion arising from the cursory and secondary search of the vehicle.¹⁹² However, such heightened privacy interest may have required more than reasonable suspicion to carry out a reasonable search.¹⁹³ As courts have stated, a person has a heightened privacy interest in the person's mobile device data,¹⁹⁴ so much so that the person may have a reasonable expectation of privacy of the mobile device data, even at the border.¹⁹⁵ Thus, the Fourth Amendment may require that a search warrant need to be obtained based on probable cause to conduct a reasonable search.¹⁹⁶

Further, Judge Wilkinson's dicta proceeds to say "[p]articularly in today's world, national security interests may require uncovering terrorist communications, which are inherently 'expressive.'"¹⁹⁷ This dicta seems to impermissibly expand Border Search Exception doctrine from its traditional limits.¹⁹⁸ Judge Wilkinson includes dicta that a warrantless search of a computer's data can be justified under the Border Search Exception doctrine to determine a person's ideology based the political climate of the time to urgently identify terrorists post 9/11.¹⁹⁹ Such dicta seems to expand the Border Search Exception doctrine significantly beyond the scope held in *Carroll*, *Ramsey*, and *Katz* of a warrantless search to determine whether a person who carries no contraband can legally enter the U.S.²⁰⁰ Further, such dicta contravenes *Ramsey*, which holds that there are instances in which a border search can be so "particularly offensive" that a warrant based on probable cause may be needed.²⁰¹ In addition, *Katz*, coupled with recent U.S. Supreme Court case law would find that a person would have a reasonable expectation of privacy to mobile device data from a border search.²⁰² Thus, any border beyond determining whether a person has a right to enter the U.S. and whether the person's belongings contain contraband may require a warrant because the border search particularly offensive for violating a person's reasonable expectation of privacy.²⁰³

United States v. Cotterman, a decision from the Ninth Circuit, also dealt with the search of mobile devices at the border.²⁰⁴ In this 2013 case, Cotterman was returning to the U.S. from Mexico.²⁰⁵ CBP officials entered his name into the Treasury Enforcement Communication System (TECS), which then indicated that Cotterman was a sex offender possibly involved with child

Carpenter, 138 S. Ct. at 2217.

¹⁹² See *Ickes*, 393 F.3d at 502.

¹⁹³ See *supra* note 11. *Ramsey*, 431 U.S. at n. 1. *Carpenter*, 138 S. Ct. at 2222.

¹⁹⁴ See *Cotterman*, 709 F.3d at 965-966; *Riley*, 134 S. Ct. at 2478-79; *Carpenter*, 138 S. Ct. at 2217.

¹⁹⁵ *Carpenter*, 138 S. Ct. at 2217.

¹⁹⁶ See *supra* note 11. *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2494-95;

Carpenter, 138 S. Ct. at 2222.

¹⁹⁷ *Ickes*, 393 F.3d at 506.

¹⁹⁸ *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13. See *Miller*, *supra* note 15, at 1953-54.

¹⁹⁹ *Ickes*, 393 F.3d at 506. See also *Iraola*, *supra* note 32 at 19-20; *Kerr*, *supra* note 7 at 295.

²⁰⁰ See *Ramsey*, 431 U.S. at 618; *Carroll*, 267 U.S. at 154. See also *Miller*, *supra* note 15, at 1953-54.

²⁰¹ See *supra* note 11. *Ramsey*, 431 U.S. at 618 n. 13.

²⁰² See *supra* note 11.

²⁰³ See *supra* note 11. *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S. Ct. at 2494-95;

Ramsey, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. 361.

²⁰⁴ *Cotterman*, 709 F.3d at 956.

²⁰⁵ *Id.* at 957.

pornography.²⁰⁶ Subsequently, CBP officials searched Cotterman's vehicle and found two laptop computers and three digital cameras.²⁰⁷ They searched the mobile devices and found several password-protected files.²⁰⁸ CBP officials detained the mobile devices for further forensic examination, after which it was revealed that the mobile devices contained over 300 files of child pornography.²⁰⁹

In Federal District Court, Cotterman moved to suppress evidence from the forensic examination based on the argument that such a search should be characterized as an "extended border search" requiring reasonable suspicion, and there was none in this case.²¹⁰ The District Court found that the TECS indication of Cotterman being a sex offender and the existence of password protected files did not amount to reasonable suspicion and granted the motion to suppress this evidence.²¹¹

On appeal, Judge McKeown stated that the Extended Border Search doctrine is a "search away from the border where entry is not apparent, but where the dual requirements of reasonable certainty of a recent border crossing and reasonable suspicion of criminal activity are satisfied."²¹² Further, Judge McKeown found the forensic examination was not an extended border search, as it did not fit the definition.²¹³

However, Judge McKeown found that "[n]otwithstanding a traveler's diminished expectation of privacy at the border, the search is still measured against the Fourth Amendment's reasonableness requirement, which considers the nature and scope of the search."²¹⁴ Further, Judge McKeown found that "the Supreme Court has recognized that the 'dignity and privacy interests of the person being searched' at the border will on occasion demand 'some level of suspicion in the case of highly intrusive searches of the person.'"²¹⁵ In addition, Judge McKeown stated, "[I]ikewise, the Court has explained that 'some searches of property are so destructive,' 'particularly offensive,' or overly intrusive in the manner in which they are carried out as to require particularized suspicion."²¹⁶ In addition, Judge McKeown cited *United States v. Ramsey* as the case in which the U.S. Supreme Court explicitly held that there may be some instances where such searches at the border would be unreasonable.²¹⁷ Judge McKeown stated the U.S. Supreme Court left "open the question of when a 'particularly offensive' search might fail the reasonableness test" as found in *Ramsey*.²¹⁸

Moreover, Judge McKeown found that a person has substantial privacy interests in the

²⁰⁶ *Id.*

²⁰⁷ *Id.*

²⁰⁸ *Id.* at 957-58.

²⁰⁹ *Id.* at 958. LaFave, *supra* note 8 at §10.5(f).959.

²¹⁰ *Cotterman*, 709 F.3d at 959.

²¹¹ *Id.*

²¹² *Id.* at 961 (quoting *United States v. Guzman-Padilla*, 573 F.3d 865, 878-79 (9th Cir. 2009)).

²¹³ *Id.*

²¹⁴ *Id.* at 963.

²¹⁵ *Id.* (quoting *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004)).

²¹⁶ *Cotterman*, 709 F.3d at 963. Kerr, *supra* note 7 at 295-96. *Id.*, (quoting *Flores-Montano*, 541 U.S. at 152, 154 n.2, 155-56, and *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985)).

²¹⁷ *Cotterman*, 709 F.3d at 963.

²¹⁸ *Id.*

information stored in their mobile devices.²¹⁹ The information stored on mobile devices can be construed as “papers” in the Fourth Amendment, which grants “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”²²⁰ Judge McKeown also stated that there is evidence that the DHS itself finds substantially more of a privacy interest by people of their mobile device data than in their belongings, such as a briefcase, which was resonated by recent U.S. Supreme Court case law.²²¹ Such evidence shows that a person has a reasonable expectation of privacy from a border search of mobile device data via DHS’s own analysis and that any border search requires a search warrant.²²²

Thus, *Cotterman* comports with *Ickes* and reaffirms *Ramsey* that the Border Search Exception doctrine limits a warrantless search to ascertaining whether a person can legally enter the U.S. and whether the person carries any contraband.²²³ Any further border search may be considered a “particularly offensive search”²²⁴ and may require a search warrant *a priori*, especially for electronic data such as mobile device data.²²⁵ In addition, Judge McKeown found any further search must carry at least some reasonable suspicion.²²⁶ However, as in *Ickes*, Judge McKeown likely did not go far enough.²²⁷ Viewing the facts not only in view of *Carroll* and *Ramsey*, but also in view of *Katz* and recent U.S. Supreme Court case law, the court should have found that a person has a reasonable expectation of privacy of its mobile device data.²²⁸ The Border Search Exception rationale implies that once a person is determined to legally enter the U.S. and carries no contraband, any further border search should comport with the *Katz* test requiring a warrant based on probable cause to be reasonable and thereby constitutional under the Fourth Amendment, otherwise it may be “particularly offensive.”²²⁹

In *United States v. Saboonchi*, a federal case in the District of Maryland, Ali Saboonchi was returning from Canada and entered the U.S. near Buffalo, New York.²³⁰ CBP officials questioned Saboonchi and entered his name into the TECS.²³¹ The TECS had two flags against Saboonchi indicating two investigations related to interactions with Iran.²³² Based on these flags,

²¹⁹ *Id.* at 964.

²²⁰ *Id.*; U.S. CONST. amend. IV.

²²¹ *Cotterman*, 709 F.3d at 965-66; *Riley*, 134 S.Ct. at 2494-95; *Carpenter*, 138 S. Ct. at 2217.

²²² *See supra* text accompanying note 11; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2494-95; *Carpenter*, 138 S. Ct. at 2217. *See also supra* note 11. *Katz*, 389 U.S. at 361.

²²³ *Cotterman*, 709 F.3d at 963. *See supra* note 11 and accompanying text; *Carroll*, 267 U.S. 132, at 153-154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2494-95.

²²⁴ *Id.*

²²⁵ *Carpenter*, 138 S. Ct. at 2222.

²²⁶ *Id.*

²²⁷ *See supra* note 11 and accompanying text; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13.

²²⁸ *See supra* note 11. and accompanying text; *Carroll*, 267 U.S. at 153-154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Carpenter*, 138 S. Ct. at 2217.

²²⁹ *See supra* note 11 and accompanying text; *Carroll*, 267 U.S. at 153-154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13.

²³⁰ *Saboonchi*, 990 F. Supp. 2d at 539-40.

²³¹ *Id.* at 539-41.

²³² *Id.* at 540.

his mobile devices, which included two mobile phones and a flash drive, were confiscated.²³³ The mobile devices were forensically searched and revealed that Saboonchi may have interned with an Iranian company.²³⁴ After further investigation of the company, it was found that Saboonchi had conducted business with the Iranian company in violation of U.S. law.²³⁵ Saboonchi moved to suppress the evidence found from the mobile devices due to a warrantless search.²³⁶

Judge Grimm analyzed the warrantless search of the mobile devices under the Border Search Exception doctrine.²³⁷ Judge Grimm stated,

I cannot help but find that even if a computer or cell phone is analogized to a closed container, a forensic search cannot be analogized to a conventional search of luggage or even of a person. A forensic search is far more invasive than any other property search that I have come across and, although it lacks the discomfort or embarrassment that accompanies a body-cavity search, it has the potential to be even more revealing.²³⁸

In addition, Judge Grimm found that “a computer forensic search is at least as invasive as an x-ray, takes longer, and reveals considerably more information.”²³⁹ Thus, Judge Grimm held “under the facts presented to me in this case, I find that a search of imaged hard drives of digital devices taken from the Defendant at the border . . . cannot be performed in the absence of reasonable suspicion.”²⁴⁰ However, Judge Grimm went on to explain in the decision that the fact that Saboonchi had two flags in the TECS, indicating he was under two investigations for dealings with Iran was reasonable suspicion for a warrantless search of the mobile devices.²⁴¹

Again, as in *Ickes* and *Cotterman*, the Border Search Exception doctrine is limited to allow for a warrantless search of a person and their belongings to determine that the person can legally enter the U.S. and carries no contraband.²⁴² Thereafter, Judge Grimm found any further search requires reasonable suspicion.²⁴³ However, as in *Ickes* and *Cotterman*, Judge Grimm may not have gone far enough.²⁴⁴ The underlying rationale of *Carroll* was that a warrantless search is only for ascertaining whether a person can legally enter the U.S. and carries no contraband.²⁴⁵ *Ramsey* finds that some border searches can be particularly offensive to the privacy interest of an individual

²³³ *Id.* at 539-541.

²³⁴ *Id.* at 540-543.

²³⁵ *Id.* at 542-543.

²³⁶ *Id.* at 540.

²³⁷ *Id.* at 544-45.

²³⁸ *Id.* at 568.

²³⁹ *Id.* at 569.

²⁴⁰ *Id.* at 569.

²⁴¹ *Id.* at 571.

²⁴² *Id.* at 545.

²⁴³ *Id.*

²⁴⁴ See *supra* note 11 and accompanying text; *Carroll*, 267 U.S. at 153-154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13.

²⁴⁵ *Carroll*, 267 U.S. at 154. See *Miller*, *supra* note 15, at 1953-54.

without providing any further guidance.²⁴⁶ However, the *Katz* test can be used to determine whether a border search is particularly offensive.²⁴⁷ Under *Katz*, one can determine whether a person has a reasonable expectation of privacy from a particular border search.²⁴⁸ Further, under the *Katz* test and recent U.S. Supreme Court case law as well as in *Cotterman* and in *Saboonchi*, the courts indicate that a person has a reasonable expectation of privacy from a border search of the person's mobile device data, thereby requiring a search warrant based on probable cause for any border search of mobile device data.²⁴⁹

III. DHS RULES CALLING FOR WARRANTLESS SEARCH OF MOBILE DEVICE DATA ARE LIKELY UNCONSTITUTIONAL

DHS has instituted rules titled "Inspection of Electronic Devices" stating that all people, baggage, and merchandise arriving in, or departing from, the United States are subject to inspection, search and detention.²⁵⁰ The inspection, search, or detention is done without a warrant.²⁵¹ The purpose of the DHS rules is for CBP officials to not only determine the identity and citizenship of all people seeking entry into the United States, but also identify and deter anyone who may be a possible terrorist from attempting to enter the country.²⁵² The DHS rules cite 8 U.S.C. § 1357 as authority for a warrantless border search.²⁵³ 8 U.S.C. § 1357 states, in pertinent part, that a CBP official "shall have power to conduct a search, without a warrant, of the person and of the personal effects in the possession of any person seeking admission to the United States of whom the CBP official may have a reasonable cause to suspect that grounds exist for denial of admission to the United States," nothing more.²⁵⁴

Moreover, applying DHS rules to identify a person having a legal right to enter the U.S. as a terrorist does not comport with the Border Search Exception doctrine held in *Carroll* and *Ramsey* in conjunction with *Katz*.²⁵⁵ That is, once CBP officials conduct a warrantless border search to determine that a person is a U.S. citizen or has the right to enter the United States, no further border search of the person's belongings to determine whether the person has a terrorist ideology should be conducted without a warrant because it may be "particularly offensive."²⁵⁶ Further, a warrantless border search of a person's mobile device data to determine whether a person has a terrorist ideology contravenes the person's reasonable expectation of privacy, thereby "particularly

²⁴⁶ *Ramsey*, 431 U.S. at 618 n. 13.

²⁴⁷ *See supra* note 11 and accompanying text; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13.

²⁴⁸ *Katz*, 389 U.S. at 361.

²⁴⁹ *Supra* note 11 and accompanying text; *Cotterman*, 709 F.3d at 965-66; *Carroll* at 267 U.S. 132, at 153-154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2494-95. *Carpenter* 138 S. Ct. at 2222.

²⁵⁰ *Inspection of Electronic Devices* U.S. CUSTOMS AND BORDER PROTECTION, *supra* note 8.

²⁵¹ *Id.*

²⁵² *Iraola*, *supra* note 32, at 20.

²⁵³ *Inspection of Electronic Devices* U.S. CUSTOMS AND BORDER PROTECTION, *supra* note 8.

²⁵⁴ 8 U.S.C. § 1357 (2006).

²⁵⁵ *See supra* note 11 and accompanying text; *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Kerr*, *supra* note 7.

²⁵⁶ *See supra* note 11 and accompanying text; *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Miller*, *supra* note 15, at 1953-54.

offensive” in view of the *Katz* test and recent U.S. Supreme Court case law in conjunction with the holdings of *Carroll* and *Ramsey*.²⁵⁷ Thus, the DHS rules are likely unconstitutional when conducting warrantless border searches of mobile device data in light of *Carroll*, *Ramsey*, and *Katz* and recent U.S. Supreme Court case law.²⁵⁸

Application of the DHS rules are currently being adjudicated to determine their unconstitutionality in warrantless border searches of mobile device data.²⁵⁹ In the events related to Sidd Bikkannavar described herein, the ACLU sued the DHS on behalf of Bikkannavar and his co-plaintiffs in *Alasaad v. Duke*, in Federal District Court in Massachusetts.²⁶⁰ The facts of the case indicate that Bikkannavar was identified by CBP officials to be a U.S. citizen and had the right to enter the United States as well as carrying no contraband.²⁶¹ The warrantless border search of Bikkannavar should have ended there.²⁶² Instead, CBP officials may have overstepped their authority by not only determine whether Bikkannavar had a right to enter the country but also determine whether or not he was a terrorist, which is “particularly offensive.”²⁶³ To that end, CBP officials conducted a warrantless border search of his mobile phone data to determine whether such data would reveal that he was a terrorist.²⁶⁴ Such a warrantless border search may violate the Fourth Amendment because it is both beyond the scope of the Border Search Exception doctrine in view of *Ramsey* and because Bikkannavar had a reasonable expectation of privacy to his mobile phone data under the *Katz* test and recent U.S. Supreme Court case law.²⁶⁵ Therefore, the border search of his mobile phone data is likely unconstitutional in view of the Fourth Amendment.²⁶⁶

In response to Bikkannavar’s complaint, the DHS filed a motion to dismiss citing that CBP officials have unbridled authority to search people and their belongings, including mobile phone data without a warrant at the border based on U.S. Supreme Court jurisprudence regarding the Border Search Exception doctrine.²⁶⁷ As is demonstrated herein, they do not.²⁶⁸

IV. U.S. SUPREME COURT HOLDS SEARCH OF MOBILE DEVICE DATA NEEDS A WARRANT

Although there has been no U.S. Supreme Court case dealing with border searches of the contents of mobile devices under the Border Search Exception doctrine, the U.S. Supreme Court

²⁵⁷ See *supra* note 11 and accompanying text; *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Carpenter*, 138 S. Ct. at 2222.

²⁵⁸ *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 36; *Ramsey*, 431 U.S. at 618 n. 13; *Carpenter*, 138 S. Ct. at 2222.

²⁵⁹ Amended Complaint, *supra* note 21, at 39.

²⁶⁰ *Id.* at 21-22, 39.

²⁶¹ *Id.* at 21-22.

²⁶² *Id.* at 39.

²⁶³ *Iraola*, *supra* note 32. See *supra* note 11 and accompanying text; *Carroll*, at 267 U.S. at 153-154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2494-95.

²⁶⁴ Amended Complaint, *supra* note 21 at 21-22. See Motion to Dismiss *supra* note 19 at 3.

²⁶⁵ *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Carpenter*, 138 S. Ct. at 2217.

²⁶⁶ Amended Complaint, *supra* note 21, at 40-41.

²⁶⁷ Motion to Dismiss, *supra* note 19.

²⁶⁸ *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13.

has dealt with the warrantless search of mobile devices incident to arrest.²⁶⁹

In *Riley v. California*, David Leon Riley was stopped by the police while driving his vehicle for expired registration tags.²⁷⁰ During the traffic stop, the police found that Riley was driving under a suspended license.²⁷¹ As a matter of standard operating procedure, the police impounded Riley's vehicle.²⁷² During an inventory search of the vehicle, police found two concealed firearms.²⁷³ Subsequently, Riley was arrested for possession of concealed firearms.²⁷⁴ Upon a search of Riley's person incident to arrest, the police seized a mobile phone as well as personal effects that indicated Riley's gang affiliation.²⁷⁵ The police searched the contents of the mobile phone and found photographs of Riley in front of a car that was involved in a shooting a few weeks earlier.²⁷⁶ Riley was charged with the earlier shooting based at least in part on the evidence found from the search of the mobile phone.²⁷⁷ Riley moved to suppress the evidence found on his mobile phone on the basis that it was found through a warrantless search.²⁷⁸ The trial court denied the motion and the California Court of Appeal affirmed.²⁷⁹

Chief Justice Roberts issued the majority opinion that stated, based on U.S. Supreme Court precedent, the purpose of a warrantless search incident to arrest is to remove any weapons that pose a threat to law enforcement and destruction of evidence.²⁸⁰ Further, Chief Justice Roberts stated that "we generally determine whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"²⁸¹ Chief Justice Roberts addressed the basis for the Search Incident to Arrest exception by stating "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."²⁸² Further, Chief Justice Roberts found that law enforcement officers can conduct a warrantless search of the mobile phone to determine that it is free of any weapons.²⁸³ However, once it is determined that the mobile phone is free of weapons, there is no need to conduct a warrantless search of the data on the mobile phone for officer safety reasons.²⁸⁴ Further, Chief Justice Roberts addressed the other aspect of the Search Incident to Arrest exception by stating "once law enforcement officers have secured a cell phone, there is no

²⁶⁹ *Riley*, 134 S.Ct. at 2480.

²⁷⁰ *Id.*

²⁷¹ *Id.*

²⁷² *Id.*

²⁷³ *Id.*

²⁷⁴ *Id.*

²⁷⁵ *Id.*

²⁷⁶ *Id.* at 2480-81.

²⁷⁷ *Id.* at 2481.

²⁷⁸ *Id.*

²⁷⁹ *Id.*

²⁸⁰ *Id.* at 2482, 85.

²⁸¹ *Id.* at 2484.

²⁸² *Id.* at 2485.

²⁸³ *Id.*

²⁸⁴ *Id.*

longer any risk that the arrestee himself will be able to delete incriminating data from the phone.”²⁸⁵

The underlying rationale of the Search Incident to Arrest doctrine is to allow a warrantless search incident to an arrest to find weapons to protect law enforcement officers and to prevent destruction of evidence.²⁸⁶ Chief Justice Roberts held in *Riley* that any further search, including the data accessible by a cell phone, required a search warrant based on probable cause because a cell phone is not simply a communication device but can be a storage device containing intimate details of a person’s life.²⁸⁷ Such intimate details are ones that should receive the utmost protection under the Fourth Amendment.²⁸⁸ Thus, Chief Justice Roberts’s holding can be interpreted to indicate that a person has a reasonable expectation of privacy of his or her mobile device data, even from a Search Incident to Arrest, an exception to the warrant requirement of the Fourth Amendment.²⁸⁹ The Search Incident to Arrest exception is analogous to the Border Search Exception doctrine, which allows a warrantless search of a person and the person’s belongings to determine whether the person can legally enter the country and whether the person’s belongings contain any contraband.²⁹⁰

Further, the rationale from *Riley* can be analogized to the rationale described herein.²⁹¹ That is, after a warrantless border search determines that a person can legally enter the U.S. and carries no contraband, the person has a reasonable expectation of privacy from a border search of the person’s mobile device data.²⁹² Any search of data accessible from the person’s mobile device may require a search warrant based on probable cause to be constitutional because such a border search contravenes the person’s reasonable expectation of privacy, which can be construed as “particularly offensive.”²⁹³

Another recent U.S. Supreme Court case, *Carpenter v. U.S.*, regarding a warrantless search of mobile device data further bolsters the assertion that mobile device data searched at the border may require a warrant.²⁹⁴ In this 2018 case, police officers arrested an accomplice of Timothy Carpenter in the robbing of several stores in Michigan and Ohio.²⁹⁵ With this information, police officers submitted court orders (not warrants) to Carpenter’s mobile phone carriers for location

²⁸⁵ *Id.* at 2486.

²⁸⁶ *Id.* at 2485-86.

²⁸⁷ *Id.* at 2494-95.

²⁸⁸ *Id.*

²⁸⁹ *Katz*, 389 U.S. at 361.

²⁹⁰ *Carroll*, 267 U.S. at 153-54, 158.

²⁹¹ *See supra* text accompanying note 11; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361; *Riley*, 134 S.Ct. at 2495.

²⁹² *See supra* text accompanying note 11.; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361; *Riley*, 134 S.Ct. at 2495; *Carpenter*, 138 S. Ct. at 2222. *See also* Miller *supra* note 15, at 1953-54.

²⁹³ *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13. *Carpenter*, 138 S. Ct. at 2222.

²⁹⁴ *See Carpenter*, 138 S. Ct. 2206, 2217 (2018) (“Allowing government access to cell-site records contravenes that ‘reasonable’ expectation. Although such records are generated for commercial purposes, that distinction does not negate Carpenter’s anticipation of privacy in his physical location. Mapping a cell phone’s location over the course of 127 days provides an all-encompassing record of the holder’s whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’ These location records ‘hold for many Americans the ‘privacies of life.’”) (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) and *Riley*, 134 S. Ct. at 2494-95).

²⁹⁵ *Id.* at 2212.

information regarding his mobile phone.²⁹⁶ Based on this obtained mobile phone location information, police officers arrested Carpenter for taking part in the robberies.²⁹⁷

Chief Justice Roberts delivered the opinion of the Court.²⁹⁸ He explained that the third party doctrine states that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”²⁹⁹ However, the Chief Justice holds that the third party doctrine does not extend to mobile device location information because “an individual maintains a legitimate expectation of privacy in the record of his physical movements.”³⁰⁰ Thus, when the police obtained Carpenter’s mobile device location information, they “invaded Carpenter’s reasonable expectation of privacy in the whole of his physical movements. Therefore, Chief Justice Roberts holds that “a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party” such as mobile device location information.³⁰¹

Parsing and deconstructing Chief Justice Roberts’ rationale in both *Riley* and *Carpenter*, and applying it to the Border Search Exception doctrine reveals a syllogism to the assertions made herein.³⁰² That is, in *Riley*, the Search Incident to Arrest is an exception to the warrant requirement.³⁰³ Chief Justice Roberts delineates the bounds of exception.³⁰⁴ The Court found a legitimate expectation of privacy of mobile device data that can be construed in applying the *Katz* test.³⁰⁵ Finally, the Court found that this legitimate expectation of privacy falls outside the narrow exception to the warrant requirement, holding that any search of the mobile device data requirement a warrant.³⁰⁶ Similarly, in *Carpenter*, Chief Justice Roberts found that although the disclosure of mobile device data to a third party invokes the Third Party Doctrine exception to the warrant requirement, the legitimate expectation of privacy in an individual’s mobile device data overrides the Third Party Doctrine exception in the disclosure of mobile device data, which can again be construed to applying the *Katz* test.³⁰⁷ Thus, the Court held that search of mobile device data requires a warrant even though it was previously disclosed to a third party.³⁰⁸ The syllogism holds for the assertions made herein.³⁰⁹ The Border Search Exception doctrine is an exception to the warrant requirement.³¹⁰ It is a narrow exception to determine whether a person can legally enter the United States or whether the person’s belonging contain contraband.³¹¹ Applying the *Katz* test

²⁹⁶ *Id.* at 2211-12. Location information of Carpenter’s mobile phone was stored at cell site locations which communicated with his mobile phone.

²⁹⁷ *Id.* at 2212.

²⁹⁸ *Id.* at 2211.

²⁹⁹ *Id.* at 2216 (quoting *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)).

³⁰⁰ *Id.* at 2217.

³⁰¹ *Id.* at 2212, 2222.

³⁰² *See supra* note 11.

³⁰³ *Riley*, 134 S.Ct. at 2485.

³⁰⁴ *Id.*

³⁰⁵ *Id.* at 2494-95

³⁰⁶ *Id.*

³⁰⁷ *Carpenter*, 136 S. Ct. 2216-17.

³⁰⁸ *Carpenter*, 136 S. Ct. 2216-17, 2222.

³⁰⁹ *See supra* note 11.

³¹⁰ *See Miller supra* note 15, at 1953-54.

³¹¹ *Id.*

shows that a person has a legitimate expectation of privacy in mobile device data.³¹² Further, border search of mobile device data falls out of the narrow exception of the rationale behind the Border Search Exception doctrine because it is “particularly offensive” for contravening a person’s reasonable expectation of privacy of his/her mobile device data.³¹³ Thus, a warrant may be required to search mobile device data at the border.³¹⁴

V. ASCERTAINING THAT A PERSON HAS RIGHT TO ENTER THE UNITED STATES DOES NOT MEAN ASCERTAINING A PERSON IS NOT A TERRORIST

Synthesizing the concepts discussed herein reveals that the Border Search Exception doctrine was promulgated to balance the public interest of the country with the privacy interests of the individual.³¹⁵ The public interest is only to ascertain that a person at the border has a right to enter the country and is not bringing any contraband into the country.³¹⁶ After which, a person’s individual privacy interest is heightened³¹⁷ and any further border search must be conducted in view of a person’s expectation of privacy.³¹⁸ If not, a warrantless border search of the person’s belongings can likely be construed as “particularly offensive”, unreasonable, and unconstitutional according to the Fourth Amendment.³¹⁹

This balanced approach to border searches has been promulgated since the inception of the Border Search Exception doctrine but has been ignored by federal courts and CBP officials in recent years.³²⁰ The Court in *Carroll*, in announcing the Border Search Exception doctrine, explicitly held 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.”³²¹ The Court did not expressly expand the Border Search Exception to any other warrantless border search, thereby setting limits to the Border Search Exception doctrine.³²² The Court reinforced the notion of the Border Search Exception doctrine limitations in *Ramsey* by stating “[w]e do not decide whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it is carried out,”³²³ but the Court did not provide any further guidance

³¹² *Carpenter*, 136 S. Ct. at 2217.

³¹³ *See supra* note 11.

³¹⁴ *Id.*

³¹⁵ *Park, supra* note 42, at 314.

³¹⁶ *Carroll*, 267 U.S. at 154; *Miller supra* note 15, at 1953-54.

³¹⁷ *See supra* text accompanying note 11; *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13. *See also* *Miller supra* note 15.

³¹⁸ *See supra* text accompanying note 11; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at n. 13. *See Miller supra* note 15, at 1996.

³¹⁹ *See supra* text accompanying note 11; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at n. 13; *Riley*, 134 S.Ct. at 2494-95. *See, e.g.*, *Kerr, supra* note 7; Amended Complaint, *supra* note 21, at 40-41.

³²⁰ *Park, supra* note 42, at 313-14. *Ickes*, 393 F.3d at 502; *Cotterman*, 709 F.3d at 957; *Saboonchi*, 990 F. Supp. 2d at 549.

³²¹ *Carroll*, 267 U.S. at 154.

³²² *Ramsey*, 431 U.S. at 618 n. 13; *Kerr, supra* note 7.

³²³ *Ramsey*, 431 U.S. at 618 n. 13. *Kerr, supra* note 7.

on which border searches are particularly offensive to require obtaining a search warrant based on probable cause.³²⁴ However, *Katz*, decided ten years prior to *Ramsey*, can provide the guidance needed to determine which border searches are particularly offensive and may require a warrant.³²⁵ That is, the confluence of *Carroll*, *Ramsey*, and *Katz*, finds that a person has a reasonable expectation of privacy from any border search that is more than ascertaining whether a person can legally enter the U.S. or carries contraband.³²⁶ Such a border search requires a warrant.³²⁷ Further, the DHS itself as well as federal courts, including the U.S. Supreme Court, find that a person has a reasonable expectation of privacy in a person's mobile device data.³²⁸ Therefore, any border search of a person's mobile device data may require obtaining a search warrant based on probable cause, otherwise such a border search may be "particularly offensive."³²⁹

Without the limit of obtaining a search warrant from a judge, there exists a risk that an overzealous CBP official will aggressively use his or her authority to search the data of a mobile device of a person entering the border under the Border Search Exception doctrine.³³⁰ For example, in the case of *Alasaad v. Duke*, even after it was determined that he had a legal right to enter the U.S. and carried no contraband, Bikkannavar had the data of his mobile phone searched without a warrant to determine whether he was a terrorist.³³¹ The warrantless border search was even more egregious because Bikkannavar had gone through two separate background checks to determine he was no security risk.³³²

As the Border Search Exception doctrine states, a warrantless border search of a person and the person's belongings is permissible to ascertain only whether the person has a right to enter the United States or whether the person's belongings contain contraband.³³³ Historically, the determination of the right to enter the United States has been limited to whether the person is a U.S. citizen, legal immigrant, or current visa holder.³³⁴ However, the DHS instituted rules that have expanded the scope of this determination to include whether a person is a terrorist.³³⁵ A terrorist is defined as a person that would commit violence against a country and/or its civilians for political cause.³³⁶ Thus, to ascertain whether a person is a terrorist at the border, CBP officials must first determine a person's political ideology and then determine that the person intends to cause acts of violence against the United States and its civilians.³³⁷ To do so, the DHS promulgated rules that

³²⁴ *Ramsey*, 431 U.S. at 618 n. 13. Kerr, *supra* note 7.

³²⁵ See *supra* text accompanying note 11; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2494-95.

³²⁶ *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 347; *Ramsey*, 431 U.S. at 618 n. 13.

³²⁷ *Carroll*, 267 U.S. at 153-54; *Katz*, 389 U.S. at 360-61; *Ramsey*, 431 U.S. at 618 n. 13.

³²⁸ *Cotterman*, 709 F.3d at 965-66; *Riley*, 134 S.Ct. at 2478-79.

³²⁹ *Katz*, 389 U.S. at 361; *Riley*, 134 S.Ct. at 2495.

³³⁰ *Iraola*, *supra* note 32. *Supra* text accompanying note 11; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2494-95. Grinberg and Croft, *supra* note 21.

³³¹ Amended Complaint, *supra* note 21, at 20-22.

³³² *Waddell*, *supra* note 40.

³³³ *Carroll*, 267 U.S. at 153-54. Miller *supra* note 15, at 1953-54.

³³⁴ *United States v. Martinez-Fuerte*, 428 U.S. 543, 555-56 (1976).

³³⁵ *Iraola*, *supra* note 32 at 3 n.10.

³³⁶ *Id.* See also FBI, WHAT WE INVESTIGATE, *supra* note 32.

³³⁷ See *Inspection of Electronic Devices*, *supra* note 8; FBI, WHAT WE INVESTIGATE, *supra* note 32 (stating

expand its powers to search the data accessible from a person's mobile devices.³³⁸ The hope is to determine a person's ideology from searching a person's email and social media content through his or her mobile phone.³³⁹ However, conducting such a warrantless border search of the person's mobile device data including personal email messages and social media is not within the scope of the Border Search Exception doctrine.³⁴⁰

Recall that the rationale of the Border Search Exception doctrine is to determine whether a person's belongings contain contraband.³⁴¹ Thus, under the rationale of the Border Search Exception doctrine, CBP officials can only conduct a warrantless border search to determine that a person's mobile phone is not contraband (for example, the cell phone does not hide a weapon or controlled substances).³⁴² Such a determination can be done by X-ray machine or other means to detect the contraband.³⁴³

However, any further warrantless border search of data accessible from the mobile phone would be beyond the scope of the Border Search Exception doctrine based on *Ramsey* and *Katz*, and bolstered by *Riley* and *Carpenter*.³⁴⁴ That is, a warrantless search of the data of the mobile phone to determine a person's ideology to further determine whether a person is a terrorist would be "particularly offensive," unreasonable, and thereby likely unconstitutional under the Fourth Amendment.³⁴⁵ To otherwise be constitutional would require a warrant from a judicial officer based on probable cause.³⁴⁶

VI. SOME OF ACADEMIA RELUCTANT TO REQUIRE A WARRANT FOR A BORDER SEARCH OF MOBILE DEVICE DATA

Review of the case law of the Border Search Exception doctrine shows that courts are reluctant to require CBP officials to obtain a warrant based on probable cause for some types of searches.³⁴⁷ Some of Academia is equally reluctant to demand that there may be a particular border search that may require a warrant based on probable cause.³⁴⁸ These academics recognize that there

terrorism is conducted by people with extremist ideology).

³³⁸ See *Inspection of Electronic Devices*, *supra* note 8; FBI, WHAT WE INVESTIGATE, *supra* note 32 (stating terrorism is conducted by people with extremist ideology).

³³⁹ See Motion to Dismiss *supra* note 19 at 3.

³⁴⁰ *Carroll*, 267 U.S. at 153-154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Carpenter*, 136 S. Ct. at 2222,

³⁴¹ *Carroll*, 267 U.S. at 153-54. Kerr, *supra* note 7.

³⁴² *Riley*, 134 S.Ct. at 2485. Miller *supra* note 15 at 1953-54.

³⁴³ *Riley*, 134 S.Ct. at 2485.

³⁴⁴ *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2485; *Carpenter*, 138 S. Ct. at 2222.

³⁴⁵ *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2495; *Carpenter*, 138 S. Ct. at 2222.

³⁴⁶ *Carroll*, 267 U.S. at 154; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618 n. 13; *Riley*, 134 S.Ct. at 2495; *Carpenter*, 138 S. Ct. at 2222.

³⁴⁷ *Ramsey*, 431 U.S. at 624; *Ickes*, 393 F.3d at 507; *Cotterman*, 709 F.3d at 970; *Saboonchi*, 990 F.Supp.2d at 571.

³⁴⁸ Park, *supra* note 42, at 312-14 (stating "this Article urges that such a [reasonable suspicion] standard

is a balance of the country's public interest and the individual privacy's interest at the border.³⁴⁹ Further, these academics recognizes that the search of mobile device data is a challenge in balancing these two interests.³⁵⁰ Some academics even recognize that *Riley* may have an impact on the search of mobile device data at the border.³⁵¹ However, academics cited herein are still reluctant to acknowledge that a border search of mobile device data may require a warrant based on probable cause because it contravenes a person reasonable expectation of privacy in his/her mobile device data, thereby being "particular offensive."³⁵² Moreover, some academics do not acknowledge that the *Katz* test should be applied to border searches, even though *Ramsey* states that some border searches can be particularly offensive to require a search warrant (despite not providing *Ramsey* any guidance on which border searches are particularly offensive).³⁵³

Instead, some academics (cited herein) focus on the characterization of border searches of a mobile device as routine or non-routine as categorized by the courts.³⁵⁴ Routine searches are cursory searches of a person or their belongings such as questioning, pat-downs, and thorough search of their belongings.³⁵⁵ Alternatively, non-routine searches are exhaustive searches, that can include strip searches, body cavity searches, and involuntary x-rays.³⁵⁶ Routine searches require no particularized suspicion while non-routine searches require some level of reasonable individualized suspicion.³⁵⁷ Further, some of the legal literature then proceeds to characterize the border search of mobile device data as a non-routine search requiring some individualized suspicion, either reasonable suspicion or probable cause, even in view of the *Riley* decision by the U.S. Supreme Court.³⁵⁸ Generally, this author found no demands in the legal literature for a warrant based on

provides the balance that is needed between the critical interests of both law enforcement and the private individual.”).

³⁴⁹ Miller, *supra* note 15. Park, *supra* note 42, at 314.

³⁵⁰ Park, *supra* note 42, at 313 (stating “[w]hile the [Cabellero] court expressed some reservations about applying the Riley standard of probable cause at the border, the court emphasized its greater concern that ‘a cell phone search threatens significant individual privacy interests,’ and reiterated the concern expressed by the Supreme Court in Riley that ‘cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.’ Thus, ‘[a]lthough Riley could be applied to a cell phone search at the border, this [c]ourt is bound by *Cotterman*.”).

³⁵¹ *Id.*; Miller, *supra* note 15 (stating “*Riley* should lead to significant changes in the digital border search doctrine. Courts should reconsider whether to extend the border search exception to digital searches, drawing on Riley’s balancing test. Riley supports the conclusion that digital searches—which can be even more intrusive than the search of one’s home—fall outside the scope of the border search exception, which is traditionally justified by the government’s interest in preventing unwanted people and contraband from entering the country.”).

³⁵² Miller, *supra* note 15 (stating “[b]ut even if courts find the border search exception applies, Riley should lead them to treat digital searches as nonroutine searches requiring reasonable suspicion or probable cause.”); Park, *supra* note 42, at 311-12 (stating “In line with these cases, this Article urges that, just as efforts to require reasonable suspicion for digital device searches”).

³⁵³ *Ramsey*, 431 U.S. at n. 13.

³⁵⁴ Park, *supra* note 42, at 288 (stating “[o]ne district court attempted to distinguish between routine and nonroutine searches by differentiating between a ‘quick look’ and an ‘exhaustive search.’”).

³⁵⁵ Miller, *supra* note 15, at 1959-1960.

³⁵⁶ *Id.* at 1960.

³⁵⁷ Park, *supra* note 42, at 288.

³⁵⁸ Miller, *supra* note 15 (stating that “But even if courts find the border search exception applies, Riley should lead them to treat digital searches as nonroutine searches requiring reasonable suspicion or probable cause.”). Park,

probable cause for border searches of mobile device data.³⁵⁹ Although some legal scholars found that U.S. Supreme Court jurisprudence regarding the Border Search Exception doctrine allowed that some searches are particularly offensive, including the border searches of mobile device data,³⁶⁰ they generally concluded that border searches required only reasonable suspicion or at most probable cause.³⁶¹ None of the cited scholars mentioned *Katz* as a guidepost in determining whether a border search of mobile device data requires a search warrant based on probable cause.³⁶²

The difference between the general academic conversation and the discussion herein is the focus on the underlying rationale of the Border Search Exception doctrine, limitations of the Border Search Exception doctrine, and a person's reasonable expectation of privacy may construe particular border searches to be "particularly offensive" and may require obtaining a warrant in view of *Katz*, and recent U.S. Supreme Court case law.³⁶³ The underlying rationale of the Border Search Exception doctrine includes determining whether a person at the border has a legal right to enter the U.S. and whether their belongings contain contraband.³⁶⁴ Once it is determined that a person can legally enter the United States and is carrying no contraband, the Border Search Exception doctrine indicates that any further search may be "particularly offensive" without obtaining a warrant based on probable cause.³⁶⁵ A person's reasonable expectation of privacy can guide which border searches are particularly offensive to require a warrant.³⁶⁶

Mobile device data is extensive and personal³⁶⁷ such that a person has a reasonable expectation of privacy to mobile device data.³⁶⁸ Any border search of mobile device data would likely require a warrant based on probable cause.³⁶⁹ *Riley* reinforces this finding by holding that search of mobile device data requires a warrant even when the mobile device is found during a Search Incident to Arrest (another exception to the Fourth Amendment search warrant requirement) and location data of a mobile device in the normal course of an investigation.³⁷⁰ However, some of the legal literature seems reluctant to make a similar claim.³⁷¹

Moreover, some legal literature even claim that the Border Search Exception doctrine allows for warrantless search of a person and their belongings to determine whether a person entering the U.S. is a terrorist.³⁷² However, as discussed herein, that is an overbroad interpretation of the Border Search Exception doctrine that should be discarded.³⁷³ The Border Search Exception

supra note 42, at 314.

³⁵⁹ Miller, *supra* note 15; Park, *supra* note 42, at 314.

³⁶⁰ Ramsey, 431 U.S. at 618 n. 13.

³⁶¹ Miller, *supra* note 15; Park, *supra* note 42, at 313-14.

³⁶² Miller, *supra* note 15; Park, *supra* note 42, at 314.

³⁶³ Carroll, 267 U.S. at 154; Carpenter, 138 S. Ct. at 2222.

³⁶⁴ *Id.* Carroll, 267 U.S. at 154. Miller, *supra* note 15. At 1953-54.

³⁶⁵ Ramsey, 431 U.S. at 618 n. 13.

³⁶⁶ *Id.*; Katz, 389 U.S. at 347.

³⁶⁷ Cotterman, 709 F.3d at 955-56.

³⁶⁸ Katz, 389 U.S. at 361; Riley, 134 S.Ct. at 2495; Carpenter, 138 S. Ct. at 2222.

³⁶⁹ Ramsey, 431 U.S. at 61 n. 13; Carpenter, 138 S. Ct. at 2222.

³⁷⁰ Riley, 134 S.Ct. at 2495; Carpenter, 138 S. Ct. at 2222.

³⁷¹ Miller, *supra* note 15; Park, *supra* note 42, at 316.

³⁷² Iraola, *supra* note 32.

³⁷³ See *supra* text accompanying note 11; Carroll, 267 U.S. at 154; Ramsey, 431 U.S. at 618 n. 13; Katz, 389

doctrine allows for a warrantless search of a person and a person's belongings to determine whether the person can legally enter the U.S. and whether the belongings contain any contraband, nothing more.³⁷⁴ Any further border search, including a border search of mobile device data to ascertain whether a person has a terrorist ideology, can infringe on the person's reasonable expectation of privacy, making the border search "particularly offensive", thereby possibly requiring a search warrant based on probable cause.³⁷⁵

VII. CONCLUSION

A border search of mobile device data should require a warrant based on probable cause.³⁷⁶ This conclusion is based on the rationale of the Border Search Exception, *Ramsey*, and *Katz* and strengthened by the *Riley* and *Carpenter* underlying.³⁷⁷ The rationale of the Border Search Exception is rooted in the idea that both the country and the individual have privacy interests.³⁷⁸ Further, the Border Search Exception balances the public interest to protect the country from imminent harm with the individual's privacy interest at the border.³⁷⁹ In addition, the Border Search Exception allows for only a warrantless search of the person and their belongings to determine whether the person can legally enter the U.S. and whether the person is carrying contraband.³⁸⁰ Once the person is determined to be able to enter the U.S. legally and it is determined that the person carries no contraband, the public interest at the border is extinguished.³⁸¹ Thereafter, the individual's privacy interest is heightened based on the person's reasonable expectation of privacy to such an extent that any further search may require a warrant based on probable cause.³⁸²

With regard to the border search of mobile device data, courts have characterized such a search as non-routine, thereby requiring some level of individualized suspicion such as reasonable suspicion or probable cause.³⁸³ However, these lower courts are reluctant, even in view of *Katz*, *Riley*, and *Carpenter* to require any higher threshold for individualized suspicion in conducting a border search.³⁸⁴ These lower courts misunderstand the Border Search Exception doctrine to mean

U.S. at 361; *Riley*, 134 S.Ct. at 2495.

³⁷⁴ *Carroll*, 267 U.S. at 154. Miller, *supra* note 15 at 1953-54.

³⁷⁵ See *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring); *Riley*, 134 S. Ct. at 2495; *Carpenter*, 138 S. Ct. at 2222.

³⁷⁶ See *supra* text accompanying note 11. (elaborating on why the existing case law supports the supposition that mobile searches should require warrants, even in the border context); *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring); *Riley* 134 S. Ct. at 2495; *Carpenter*, S. Ct. 136 at 2222.

³⁷⁷ See *Ramsey*, 431 U.S. at n. 13; *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring); *Riley*, 134 S. Ct. at 2495. Kerr, *supra* note 7; *Carpenter*, 138 S. Ct. at 2222.

³⁷⁸ See Park, *supra* note 42 at 281.

³⁷⁹ *Carroll* 267 U.S. at 154. Park, *supra* note 42 at 281.

³⁸⁰ *Carroll* 267 U.S. at 154.

³⁸¹ See *supra* text accompanying note 11; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361; *Riley*, 134 S.Ct. at 2494-95.; Miller *Supra* note 15 at 1953-54.

³⁸² See *supra* text accompanying note 1; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 361; *Riley*, 134 S.Ct. at 2494-95.; *Carpenter*, 138 S. Ct. at 2222.

³⁸³ See *Cotterman*, 709 F.3d 952 at 961, 968.

³⁸⁴ Park, *supra* note 42, 313 (stating that a lower court would like to follow the legal rationale in *Riley* in ruling on whether a warrantless border search of mobile device data is constitutional but feel bound by the holding in

that CBP officials have almost unbridled authority to search a person and their belongings at the border in the name of the national security.³⁸⁵

Instead, the underlying rationale of the Border Search Exception holds that once it is determined that a person can legally enter the U.S. and their belongings including the mobile device, any further border search, especially a warrantless border search of a person's mobile phone data, would be an infringement on the person's reasonable expectation of privacy resulting in the border search to be "particularly offensive."³⁸⁶ Therefore, although the U.S. Supreme Court has opined that the Border Search Exception has limits without providing guidance, established Fourth Amendment jurisprudence and recent U.S. Supreme Court case law provides the guidance that may require CBP officials to obtain a warrant based on probable cause prior to conducting a border search of mobile device data.³⁸⁷ Failure to do so would likely be unconstitutional.³⁸⁸

Cotterman). See *United States v. Caballero*, 178 F. Supp. 3d 1008, 1014 (S.D. Cal. 2016) (stating that the court wished to apply *Riley*, but that it was bound by *Cotterman*); *United States v. Ramos*, 190 F. Supp. 3d 922, 1002 (S.D. Cal. 2016) ("Adopting the reasonable suspicion standard currently used only for forensic examinations of digital devices . . . as the standard for all border searches of cell phones, may be a prudent way to harmonize *Riley*'s concerns with the salutary border search principles").

³⁸⁵ See *supra* text accompanying note 11.; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 360-61; *Riley*, 134 S.Ct. at 294-95. See Motion to Dismiss *supra* note 19 at 3.

³⁸⁶ See *supra* text accompanying note 11; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at n. 13; See *Katz*, 389 U.S. at 360-61; *Riley*, 134 S. Ct. at 294-95; *Carpenter*, 138 S. Ct. at 2222.

³⁸⁷ See *supra* text accompanying note 11; *Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 360-61; *Riley*, 134 S. Ct. at 294-95; *Carpenter*, 138 S. Ct. at 2222.

³⁸⁸ *Ramsey*, 431 U.S. at 618 n. 13; *Katz*, 389 U.S. at 360-61; *Riley*, 134 S. Ct. at 2495; *Carpenter*, 138 S. Ct. at 2222.