Catholic University Journal of Law and Technology

Volume 27
Issue 2 *Spring 2019*

Article 8

2019

Warrantless Searches of Electronic Devices at U.S. Borders: Securing The Nation or Violating Digital Liberty?

Ahad Khilji
Catholic University of America (Student)

WARRANTLESS SEARCHES OF ELECTRONIC DEVICES AT U.S. BORDERS: SECURING THE NATION OR VIOLATING DIGITAL LIBERTY?

Ahad Khilji[*]

"Sorry, this media file doesn't exist on your internal storage."[1] This was the message Ghassan Alasaad saw on his phone when he tried to view videos from his daughter's graduation.[2] Unbeknownst to Mr. Alasaad, U.S. Customs and Border Protection ("CBP") searched and seized his phone two weeks prior.[3]

The steady increase of U.S. citizens traveling with smart phones and other electronic devices has been met with the rise of searches and seizures by CBP officers at U.S borders.[4] In July 2017, Ghassan and Nadia Alasaad were traveling to Massachusetts with their eleven year old daughter who was ill, with a high fever.[5] The family was returning from their vacation in Quebec when CBP officers approached them at the Highgate Springs crossing in Vermont.[6] After

[*] J.D. Candidate, May 2019, The Catholic University of America, Columbus School of Law; B.A. 2013, The Catholic University of America. The Author is grateful to Professor Daniel M. Zachem for serving as his expert reader in the research and writing of this comment. The Author would like to thank his loving and supportive parents, Dr. Nasir Mahmood Khilji and Ghazala Khilji, and his three sisters Sofia, Charmine and Michelle. Additionally, the Author would like to thank the hard work and dedication of the editors and associates of *Catholic University's Journal of Law and Technology* in preparation of this Comment.

1 *Alasaad v. Nielsen: Plaintiffs' Stories*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/alasaad-vs-duke-bios (last visited Apr. 17, 2019).

2 *Id*.

3 *Id*.

4 *See* Alasaad v. Nielsen, No. 17-cv-11730-DJC, 2018 WL 2170323, at *2 (D. Mass. May 9, 2018) (explaining CBP conducted nearly twice as many searches in the first half of 2017 than it did in all of 2015); *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile.

5 *Alasaad*, 2018 WL 2170323, at *5.

6 *Id*.; *Ghassan and Nadia Alasaad*, ACLU, https://www.aclu.org/bio/ghassan-and-

leading the family to the secondary inspection area, officers interrogated Mr. Alasaad while searching through his phone.[7] Concerned with his daughter's health, Mr. Alasaad, a naturalized U.S. citizen and limousine driver, asked why officers detained and searched his family, to which a CBP supervisor curtly replied that he simply felt like putting the Alasaad family through a secondary inspection.[8] The CBP officers then demanded that Nadia Alasaad provide the password for her locked phone.[9] Mrs. Alasaad, also a naturalized U.S. citizen and nursing student, objected on religious grounds.[10] As a Muslim she always wears a hijab when in public, and did not want officers to see photos of her without a hijab, which her phone contained.[11] After the officers threatened to confiscate the phone if she did not provide the password, Ms. Alasaad reluctantly adhered to their insistence.[12] Due to the nature of the photos, Ms. Alasaad also requested a female officer search her phone, however she was informed that providing a female officer would cause hours of further delay.[13] Exhausted from their trip and detainment, and concerned about their daughter's worsening health, the Alasaad family was forced to depart, leaving their phones with the CBP officers.[14]

Stories like the Alasaad family's that involve coercive tactics and arbitrary use of force by CBP officers are unfortunately common.[15] In the early 2000s, Americans were restricted to the usage of the Internet at a desktop computer in the home or office, requiring an immobile Internet connection, or dial up modem device to connect.[16] Beginning in the late 2000s, the United States underwent a radical departure from this outdated Internet lifestyle.[17] Smartphones and mobile devices are constantly being replaced by consumers with their newer counterpart versions; the majority of Americans are now connected to the Internet while traveling.[18]

Today 95% of Americans own some kind of cellular device.[19] The percentage of Americans who own smartphones has increased significantly from 35% in

---

nadia-alasaad (last visited Apr. 10, 2019).

7 *Alasaad*, 2018 WL 2170323, at *5.

8 *Id*.; ACLU, *supra* note 6.

9 *Alasaad*, 2018 WL 2170323, at *5.

10 *Id*.; ACLU, *supra* note 6.

11 ELEC. FRONTIER FOUND., *supra* note 1.

12 *Id*.

13 *Id*.

14 *Id*.

15 Alasaad v. Nielsen, No. 17-cv-11730-DJC, 2018 WL 2170323, at *5-8 (D. Mass. May 9, 2018).

16 PEW RES. CTR., *supra* note 4.

17 *Id*.

18 *Id*.

19 *Id*.

2011 to 77% in 2018.[20] While most Americans own cellphones and belong to a wide range of demographic groups, ownership of smart phones is often reflective of one's education, income and age.[21] Mobile phones are not the only information devices that Americans own.[22] Almost 75% of adults living in the United States own desktop or laptop computers, while approximately 50% own tablets, and 20% own e-reader devices.[23] While Americans have started to opt out of traditional broadband services, the smartphone has been cited as the increasingly main source of Internet access.[24] Almost 20% of Americans receive Internet access from just their smartphones.[25] The primary use of smartphones among lower-income Americans, minorities, and young adults is for Internet access.[26]

The Federal Aviation Administration ("FAA") has defined a Portable Electronic Device ("PED") as "any piece of lightweight, electrically-powered equipment."[27] The FAA further provides that these "devices are typically consumer electronics devices functionally capable of communications, data processing and/or utility."[28] A September 2013 report by the FAA stated that almost 94% of all U.S. adult passengers on airlines have traveled with at least one PED in a one-year period of time.[29] While passengers may place PEDs in their checked baggage, the majority of PEDs have been brought onto the plane in a carry-on item.[30] The report lists cellphones, smartphones, laptops and notebooks as the most common group of PEDs carried onto an aircraft, and frequently searched by airport personnel.[31]

In April 2017, CBP released a report relating to electronic device searches at the U.S. borders.[32] Although only less than 0.1% of all travelers may actually be subjected to a search while entering the United States, when comparing the

---

20 *Id*.

21 *Id*.

22 *Id*.

23 *Id*.

24 *Id*.

25 *Id*.

26 *Id*.; *see also* Jodie Griffin, *Universal Service in an All-IP World*, 23 COMMLAW CONSPECTUS 346, 350 (2015) (discussing policy on universal internet access for everyone, including Americans with low-income, disabilities, and rural area residents).

27 *Fact Sheet – Portable Electronic Devices Aviation Rulemaking Committee Report*, Federal Aviation Administration, https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=15255 (Oct. 31, 2013).

28 FED. AVIATION ADMIN., RECOMMENDATIONS ON EXPANDING THE USE OF PORTABLE ELECTRONIC DEVICES DURING FLIGHT 3 (2013).

29 *Id*.

30 *Id*.

31 *Id*.

32 Press Release, U.S. Customs and Border Prot., CBP Releases Statistics on Electronic Device Searches (Apr. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0.

statistics between a six month period (October-March) in 2016 with the same period in 2017, electronic device searches have almost doubled from 8,383 to 14,993.[33] Approximately one million travelers to the U.S. are inspected by the CBP every day.[34] Out of this population, nearly 2,500 electronic devices are searched on a monthly basis since October 2016.[35] Visitors, permanent residents, and even U.S. citizens' electronics may be subject to a search by CBP.[36]

This Comment will first examine the constitutionality of warrantless searches of electronic devices at United States borders, a developing and fascinating legal controversy which magnifies the broader debate between collective security and individual privacy. The courts have not fully determined whether a U.S. citizen's electronic device can be searched at the border or airport. Then, Section II of this Comment provides a background of the two conflicting views in the current debate regarding warrantless searches at the border. Section III addresses the Fourth Amendment of the United States Constitution and provides background and context to the issue of whether warrantless searches of electronic devices are constitutional. Next, Section IV explores the origin and development of both CBP and ICE under the Department of Homeland Security ("DHS"). Additionally, Section V examines the case, *Alasaad v. Nielsen* and provides an analysis of how the court should rule on the request by plaintiffs that border officers should have probable cause and secure a warrant before searching and confiscating electronic devices. Although the plaintiffs also allege a First Amendment violation,[37] this Comment will only explore the Fourth Amendment implications surrounding this case. Next, Section VI investigates the disproportionate amount of Muslims that are randomly inspected and questioned at the border and how the current presidential administration's bias towards Muslims have coincided and enforced this arbitrary screening method. Section VII will examine alternatives other than adhering or attacking the policies of CBP or ICE. Rather, this section will argue that individuals can choose to prevent themselves from becoming possible victims of arbitrary searches by following tips and advice on traveling with electronic devices. Finally, Section VIII of the Comment will recommend that the U.S. District Court of

---

33 *Id*.
34 *Id*.
35 *Id*.
36 *Id*.
37 ELEC. FRONTIER FOUND., *supra* note 1 (discussing allegations of how plaintiffs' rights were violated); Complaint for Injuctive and Declaratory Relief (Violation of First and Fourth Amendment rights) at 11, Alasaad v. Nielsen, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017) (arguing that "searches of electronic devices also impinge on constitutionally protected speech and associational rights, including the right to speak anonymously, the right to private association, the right to gather and receive information, and the right to engage in newsgathering.").

Massachusetts rule in favor of the Alasaad family and other plaintiffs by issuing an order of injunctive and declaratory relief against the unlawful warrantless searches and seizures of the DHS, CBP and ICE.

I. TWO CONFLICTING VIEWS OF THE CONSTITUTIONALITY OF BORDER SEARCHES

Proponents of these warrantless searches and seizures are the U.S. Federal Government and its Executive Agencies.[38] These searches began under President George W. Bush and became more prevalent during The Obama Administration.[39] From October 2016 to March 2017, there were approximately 15,000 searches, compared to the 8,383 conducted in the year prior.[40] During these searches, officers are known to search through social media, messages, photos, emails and private files.[41] CBP officers allege the purpose of these searches is to secure our nation's borders by locating and combating terrorism, exporting control violations, intellectual property rights infringement, and child pornography.[42] The CBP's slogan succinctly captures its policy, stating, "Securing America's Border".[43] Similarly, the U.S. Immigration and Customs Enforcement ("ICE") slogan is "Protecting National Security and Upholding Public Safety."[44] In response to criticism, the ICE and CBP have said they are required to search electronic devices by the same laws that authorize officers to search suitcases at the border without a warrant.[45] ICE and CBP have also stated that the searches are not common and only happen to "fewer than one-hundredth of one percent of international travelers."[46] According to John Wagner, a commissioner at CBP, "border searches of electronic devices are essential to enforcing the law at the U.S. border and to protecting the American people."[47] Proponents also utilize case law to bolster their argument.[48] Courts have

---

38 Daniel Victor, *Forced Searches of Phones and Laptops at U.S. Border Are Illegal, Lawsuit Claims*, N.Y. TIMES (Sept. 13, 2017) https://www.nytimes.com/2017/09/13/technology/aclu-border-patrol-lawsuit.html.

39 *Id*.

40 *Id*.

41 Chris Megerian & Brian Bennett, *U.S. dramatically increased searches of electronic devices at airports in 2017, alarming privacy advocates*, L.A. TIMES (Jan. 5, 2018), http://www.latimes.com/politics/la-na-airport-search-devices-20180105-story.html.

42 Victor, *supra* note 38.

43 *About CBP*, U.S. CUSTOMS AND BORDER PROT., https://www.cbp.gov/about (last visited Feb. 10, 2018).

44 *Who We Are*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, https://www.ice.gov/about (last visited Apr. 10, 2019).

45 Victor *supra* note 38.

46 *Id*.

47 Megerian & Bennett, *supra* note 41.

48 *Id*.

continuously held that although the Fourth Amendment protects citizens from unreasonable searches, this can be outweighed in favor of the compelling government interest in preventing crime and terrorism.[49] According to Stewart Baker, an expert on national security law and a senior policy official at DHS from 2005-2009, "The basic principle is that however personal something is, it is subject to search at the border because it is necessary to decide whether to admit people and determine if they are carrying contraband."[50]

However, privacy activists outright reject the stance that advocates of the searches have taken.[51] Opponents of warrantless searches of electronic devices argue that the border search exception to the Fourth Amendment was created in reference to luggage and only permits law enforcement to search containers at the border, not electronic devices.[52] While privacy advocates concede that protecting the border is important for national security, they argue that an American citizen or permanent resident crossing the border should have the same rights, if not more than a person arrested for allegedly committing a crime.[53] Privacy Law Professor, Ryan Calo states that warrantless searches are invasive for all travelers, but especially for U.S. citizens because these actions are what "the 4th Amendment was designed to protect against, which is arbitrary dragnet surveillance."[54] Criticisms of these searches have also come from past government representatives.[55] James Norton, a senior official at DHS during the George W. Bush administration, described device searches of American citizens as "problematic" and symbolic of a "mission creep."[56]

Another concern with warrantless searches of electronic devices is that any data or information customs officers seize and subsequently copy becomes vulnerable to hackers.[57] This problem is even more troublesome given the federal government's past failure in protecting private information.[58] Unlike

---

49 *Id*.

50 *Id*.

51 Victor, *supra* note 38.

52 *Id*. (distinguishing devices in the context of the search-incident-to-arrest exception to the warrant requirement).

53 Megerian & Bennett, *supra* note 47.

54 *Id*.

55 *Id*.

56 *Id*.; *see also* JEFFREY W. SEIFERT, CONG. RESEARCH SERV., RL31798, DATA MINING: AN OVERVIEW 12 (2004) (defining mission creep as "the use of data for purposes other than that for which data was originally collected.").

57 Megerian *supra* note 47.

58 *Id*.; *see generally* Nate Lord, *Top 10 Biggest Government Data Breaches of All Time in the U.S.*, DIGITAL GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time (discussing the various data breaches experienced by the U.S. government and the private information that was exposed, including the largest breach in which a voter database was accessed and information on 191

outdated technology such as flip phones, smart phones and electronic devices hold a vast amount of personal information or data. Cellphones containing all of this data act as a portal into the private life of their users.[59] Privacy activists argue that this vast amount of sensitive information was not intended to be subjected to warrantless searches.[60] When border officials search through a smart phone or any electronic device, it essentially allows them to improperly intrude into someone's entire life.[61] Nathan Wessler, an attorney for the American Civil Liberties Union ("ACLU"), observed that searching devices not only affects the individual traveler, but everyone the traveler has ever communicated with as well, which in effect reduces the overall security and trust of electronic information.[62] Wessler emphasizes the negative effect on the U.S. tourism industry by asking: "what traveler is going to want to lay bare every intimate detail of their social media history, exposing years of their lives?"[63]

Alasaad v. Nielsen is a case arising out of the United States District Court for the District of Massachusetts, which has exemplified the debate of warrantless searches of devices at the border.[64] The Electronic Frontier Foundation ("EFF") and the ACLU filed the lawsuit against DHS, as well as CBP and ICE, over warrantless border searches.[65] The two organizations represent eleven plaintiffs, including the Alasaad family, who had their smartphones and computers seized and searched by border agents without any kind of warrant, probable cause or reasonable suspicion.[66] Ten of the plaintiffs are U.S. citizens and one of them is a permanent resident.[67] The diverse plaintiff group includes veterans, students,

---

million Americans was exposed).

59 Riley v. California, 134 S. Ct. 2473, 2489 (2014) (explaining how the vast amount of information stored on a cell phone can be aggregated to give a person a view into an individual's private life); Dustin Volz & Nat'l Journal, *The Supreme Court Is About to Decide the Future of Cell-Phone Privacy*, THE ATLANTIC (Apr. 28, 2014), https://www.theatlantic.com/technology/archive/2014/04/the-supreme-court-is-about-to-decide-the-future-of-cell-phone-privacy/361332.

60 Volz & Nat'l Journal, *supra* note 59.

61 *Id*.

62 Andy Greenberg, *A GUIDE TO GETTING PAST CUSTOMS WITH YOUR DIGITAL PRIVACY INTACT*, WIRED (Feb. 12, 2017, 7:00 AM), https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact.

63 *Id*.

64 Alasaad v. Nielsen, No. 17-cv-11730, 2018 WL 2170323, at *1 (D. Mass. May 9, 2018); *see also ALASAAD V. NIELSEN: CHALLENGE TO WARRANTLESS PHONE AND LAPTOP SEARCHES AT U.S. BORDER*, ACLU, https://www.aclu.org/cases/alasaad-v-nielsen-challenge-warrantless-phone-and-laptop-searches-us-border (last updated Apr. 20, 2019).

65 *Alasaad*, 2018 WL 2170323, at *1; ACLU, *supra* note 64.

66 *Alasaad*, 2018 WL 2170323, at *1; ACLU, *supra* note 64.

67 Taylor Hatmaker, *Trump administration sued over warrantless smartphone searches at US borders*, TECHCRUNCH (Sept. 13, 2017), https://techcrunch.com/2017/09/13/alasaad-v-duke-eff-aclu-dhs-warrantless-searches/.

journalists, and an engineer for NASA, each of whom were returning to their home in the U.S. after traveling overseas.[68] Although none of the plaintiffs were accused of any specific crime or violation, some of them had their smartphones held for months by border officials.[69]

ACLU attorney, Esha Bhandari commented on the case stating: "electronic devices contain massive amounts of information that can paint a detailed picture of our personal lives, including emails, texts, contact lists, photos, work documents, and medical or financial records."[70] Bhandari goes on to state that "the Fourth Amendment requires that the government get a warrant before it can search the contents of smartphones and laptops at the border."[71] The Alasaad family reached out to Jessie Rossman, an attorney for the Massachusetts chapter of the ALCU, after their humiliating experience at the border.[72] Rossman explained that the Alasaads, as well as the other plaintiffs, are not seeking financial compensation.[73] Instead, the plaintiffs want the court to prevent future searches and seizures of electronic devices without a warrant, probable cause or reasonable suspicion.[74] Therefore, their complaint calls for both declaratory judgment and injunctive relief; to ask the government to stop the practice of these searches and hold such warrantless searches as unlawful and unconstitutional.[75] Rossman highlights, "What is important to emphasize about phones is that our phones have become blueprints for our entire lives . . . a cellphone is not a suitcase."[76]

II. FOURTH AMENDMENT AND THE BORDER SEARCH EXCEPTION

The Fourth Amendment of the United States Constitution prohibits unreasonable searches and seizures. It states as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon

---

68 *Id*.
69 *Id*.
70 *Id*.
71 *Id*.
72 Jess Aloe, *Couple detained at Vermont border crossing sue government over warrantless phone search*, BURLINGTON FREE PRESS (Sept. 13, 2017), https://www.burlingtonfreepress.com/story/news/2017/09/13/couple-detained-vermont-border-crossing-sue-government-over-warrantless-phone-search/654673001.
73 *Id*.
74 *Id*.
75 Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment rights), *supra* note 37, at 4; Aloe, *supra* note 72.
76 Aloe, *supra* note 72.

> probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[77]

The Fourth Amendment and its interpretation remains a central issue in criminal law as well as privacy law, providing guidance on law enforcement and their duties and responsibilities.[78] Along with protecting citizens against capricious arrests, it is the foundation governing different forms of law enforcement surveillance, search warrants, wiretaps, safety inspections, and the stop-and-frisk.[79]

When plaintiffs invoke their rights under the Fourth Amendment, providing that their rights thereunder have been violated in a case, the first issue is whether in fact a "search" actually occurred.[80] In *Katz v. United States*,[81] the Supreme Court ruled that a "search" had occurred when a microphone was placed on top of a telephone booth, which was being used by the defendant.[82] The Court found that defendant Charles Katz had an expectation of privacy when he closed the door of the phone booth, and the court determined that society has generally deemed this type of behavior as a "reasonable expectation of privacy."[83] The majority opinion, in which Justice Harlon concurs, formulated the reasonable expectation test in order to determine whether the Government has conducted a search.[84] This test was later applied in *Smith v. Maryland*,[85] where the Supreme Court held that if an individual "has exhibited an actual (subjective) expectation of privacy," and "society is prepared to recognize that this expectation is (objectively) reasonable, then there is a right of privacy in the given circumstance."[86]

The Fourth Amendment also protects people against brief detentions.[87] In *United States v. Mendenhall*,[88] the Court found that a seizure of a person occurs only when they must submit to the show of force or authority.[89] However, in *Florida v. Bostick*,[90] the Supreme Court ruled that a "seizure" under the Fourth Amendment does not occur during "citizen encounters" or in the event that law

---

77 U.S. CONST. AMEND. IV, §3.

78 Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 865 (2004).

79 *Id*. at 865-66.

80 Katz v. United States, 389 U.S. 347, 354 (1967).

81 *Id*. at 348.

82 *Id*. at 353.

83 *Id*.

84 *Id*. at 361.

85 Smith v. Maryland, 442 U.S. 735, 737 (1979).

86 *Id*. at 739-41.

87 United States v. Mendenhall, 446 U.S. 544, 551 (1980).

88 *Id*. at 553.

89 *Id*.

90 Florida v. Bostick, 501 U.S. 429, 434 (1991).

enforcement does not require individuals to comply with their requests.[91] In this case,[92] officers approached Defendant Terrance Bostick who was riding on a bus and asked him to produce his bus ticket and license.[93] The officers told Bostick that they were looking for narcotics and asked him if they could search his luggage.[94] After receiving Bostick's permission and searching his bag, the officers found cocaine and arrested him.[95] The Court in *Florida* held that the search of the bag was reasonable and permitted because Bostick could have declined the officers' request and left the bus on his own accord.[96] Therefore, if an individual can choose to not answer questions by law enforcement there has not been an intrusion or seizure of that person.[97]

For purposes of determining whether an individual's Fourth Amendment rights have been violated, a "seizure" has occurred when an individual has been arrested and taken into police custody.[98] However, law enforcement is authorized to briefly "seize" an individual when they believe that the individual is connected to a crime, also known as a "*Terry* stop."[99] In *Terry v. Ohio,*[100] the Supreme Court held officers may perform a limited search of a suspect's outer garments in order to locate weapons only if they have a "reasonable and articulable" suspicion that the individual detained may have a weapon due to the nature of the suspected crime.[101]

Reasonable suspicion requires law enforcement to have "specific and articulable facts" that the individual is about to engage in a crime.[102] Reasonable suspicion is a lower standard than probable cause, which is the high standard required to arrest someone or obtain a search warrant. Additionally, whether reasonable suspicion exists also depends on the "totality of the circumstances," which is the combination of factors regarding the specific incident.[103] Probable cause for an arrest requires that law enforcement have "the facts and circumstances within their knowledge and of which they had reasonably trustworthy information," which would cause a reasonable person to believe that

---

91 *Id*.
92 *Id*. at 431-32.
93 *Id*.
94 *Id*.
95 *Id*.
96 *Id*. at 437-38.
97 *Id*.
98 Terry v. Ohio, 392 U.S. 1, 16 (1968).
99 *Id*. at 16-17.
100 *Id*. at 17.
101 *Id*.
102 *Id*. at 27.
103 *Id*.

the individual was involved or is involved in a crime.[104] The Fourth Amendment requires that in order to be valid, a warrant must establish probable cause that the search will lead to contraband, or will uncover criminal activity.[105] Generally, officers must have legally sufficient reasons to believe a search is necessary.[106]

Under the Fourth Amendment, warrantless searches are usually unreasonable, unless an established exception is applicable.[107] Established by the First Congress of the United States of America, the border search doctrine is arguably the most fundamental and established exceptions within the Constitution.[108] This exception permits searches and seizures at U.S. borders without probable cause or a warrant.[109] Border searches are not similar to inventory searches or administrative searches because they are not searching for evidence that will justify the detaining of travelers and eventual arrests.[110] Rather, searches are deemed "routine," or "non-routine" depending on the intrusiveness of the search.[111] Accordingly, a routine border search does not offend or pose a serious invasion of privacy on the individual.[112] In the past this type of border search has involved a pat-down for weapons or contraband,[113] the use of a drug-sniffing dog[114], the removal of jackets, shoes, or hats or the emptying of purses, wallets and pockets[115], and the x-ray of objects.[116]

In *Florida v. Bostick*,[117] the Court ruled that because an individual can choose what items they bring with them while traveling the individual therefore has a chance to lower the level of intrusion they experience at the border.[118] Courts tend to examine the particular technique, mainly the degree of intrusiveness or

---

104 Beck v. Ohio, 379 U.S. 89, 91 (1964).

105 Carroll v. United States, 267 U.S. 132, 161 (1925).

106 *Id*.

107 YULE KIM, CONG. RES. SERV., RL31826, PROTECTING THE U.S. PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT 7 (2009).

108 Act of July 31, ch.5 §§ 23-24, 1 Stat. 29, 43 (1789) (current version at 19 U.S.C. §§482, 1582); KIM, *supra* note 107.

109 United States v. Ramsey, 431 US 606, 616-19 (1977).

110 KIM, *supra* note 107.

111 *Id*.

112 United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993); KIM, *supra* note 107, at 9.

113 *See* United States v. Beras, 183 F.3d 22, 24 (1st Cir. 1999) (holding that a pat-down was not intrusive enough and was instead considered to be a routine search); KIM, *supra* note 107, at 9.

114 United States v. Kelly, 302 F.3d 291, 294-95 (5th Cir. 2002); KIM, *supra* note 107, at 9.

115 United States v. Sandler, 644 F.2d 1163, 1169 (5th Cir. 1981); KIM, *supra* note 107, at 9.

116 United States v. Okafor, 285 F.3d 842, 844 (9th Cir. 2002); KIM, *supra* note 107, at 9.

117 Florida v. Bostick, 501 U.S. 429, 434-35 (1991).

118 *Id*. at 437; KIM, *supra* note 107, at 10.

invasiveness, in order to decide the classification of a search as routine or non-routine.[119] In *United States v. Braks,*[120] the court evaluated six factors for their analysis:

> (1) whether the search results in exposure of intimate body parts or requires the suspect to disrobe; (2) whether physical contact between Customs officials and the suspect occurs during the search; (3) whether force is used to effect the search; (4) whether the type of search exposes the suspect to pain or danger; (5) the overall manner in which the search is conducted; and (6) whether the suspect's reasonable expectations, if any, are abrogated by the search.[121]

In *United States v. Ramsey,*[122] the defendants were involved in a heroin drug ring whereby the defendants utilized the mail to transport heroin into the United States.[123] In New York, a customs inspector intercepted eight envelopes that were heavier and thicker than typical airmail.[124] The inspector believed the envelopes contained illegal narcotics and opened them finding the heroin as he initially suspected.[125] The customs inspector then sent the letters to the Drug Enforcement Administration ("DEA") in Washington D.C, and the letters were then opened by agents without a warrant but on the mere suspicion that the envelopes contained drugs.[126] The Supreme Court held that the search of the envelopes did not violate the Fourth Amendment and instead was a routine search that did not require probable cause or a warrant.[127] In the majority opinion, Chief Justice Rehnquist wrote "searches made at the border, pursuant to the long-standing 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."[128]

Courts have defined a non-routine search as any time an official conducting the search goes beyond a limited intrusion.[129] This type of search strays further away from a routine search and involves a combination of "strip searches, cavity searches, x-ray examinations" and the prolonged detention of an individual.[130]

---

119 KIM, *supra* note 107, at 10.
120 United States v. Braks, 842 F.2d 509, 511-12 (1st Cir. 1988).
121 *Id.*; KIM, *supra* note 107, at 10.
122 United States v. Ramsey, 431 US 606, 609-11 (1977).
123 *Id.*
124 *Id.*
125 *Id.*
126 *Id.*
127 *Id.*
128 *Id.* at 616.
129 KIM, *supra* note 107, at 10.
130 *See* United States v. Reyes, 821 F.2d 168, 170-71 (2d Cir. 1987) (labeling a strip search as non-routine); *see* United States v. Adenkunle, 2 F.3d 559, 562 (5th Cir. 1993) (x-

Further, the law demands government officials to have at least a reasonable suspicion of criminal activity in order to subject an individual to a non-routine search.[131] This standard typically requires an official to have "a particularized and objective basis for suspecting the particular person" of illegal activity.[132] In *United States v. Forbicetta*,[133] the Court held that reasonable suspicion existed when officials had observed the following facts: (1) the suspect arrived from Bogota, Colombia, (2) the defendant was by herself, (3) she only carried one bag and did not have any items that would require further inspection, (4) she was attractive, and (5) she was wearing a loose-fitted garb.[134] However, courts have rejected the argument that arriving from a specific country or location could alone provide reasonable suspicion without the support of other factors.[135]

The Supreme Court has not stated what level of suspicion is required for non-routine searches, nor have they articulated what factors are required to label a search as routine or non-routine.[136] This dilemma was partially resolved in *United States v. Montoya de Hernandez*,[137] where the Supreme Court addressed the "clear indication" standard.[138] In this case, the Court concluded that "clear indication" was in fact not a third standard, instead it is merely a term used to specify the requirement for particularized suspicion.[139] Therefore, the standard held widely by the courts for non-routine searches is reasonable suspicion.[140]

III. CBP AND ICE SEARCH AND SEIZURE FAIL TO SUFFICIENTLY PROTECT THE PRIVACY RIGHTS OF TRAVELERS

After the September 11th, 2001 terrorist attacks, the United States Government reformed national security and border control policies to restrict who was allowed in the country.[141] In March 2003, President George W. Bush created the DHS in order to unite different agencies tasked with protecting the

---

ray examination and continued detention); KIM, *supra* note 107, at 10.

131 United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985); KIM, *supra* note 107, at 10.

132 *See Montoya de Hernandez*, 473 U.S. at 541 ("the police officer must be able to point to specific and articulable facts.") (citing Terry v. Ohio, 392 U.S. 1, 21 (1968)); KIM, *supra* note 107, at 11.

133 U.S. v. Forbicetta, 484 F.2d 645, 646-47 (5th Cir. 1973).

134 *Id.*; KIM, *supra* note 107, at 11.

135 Reid v. Georgia, 448 U.S. 438, 441 (1980); KIM, *supra* note 107, at 11.

136 *Montoya de Hernandez*, 473 U.S. at 541 n.4.

137 *Id.*

138 *Id.*

139 *Id.* at 533.

140 *Id.* at 541.

141 Willa Frej, *How U.S. Immigration Policy Has Changed Since 9/11*, HUFFINGTON POST (Sept. 9, 2016), https://www.huffingtonpost.com/entry/us-immigration-since-911_us_57d05479e4b0a48094a71bc0.

nation.[142] Within the DHS, the three main agencies consist of CBP, ICE and U.S. Citizenship and Immigration Services ("USCIS").[143] The post 9/11 duties of these agencies include cooperating and communicating information with other countries, requiring further screenings and interviews with people of certain backgrounds, and collecting information on international travelers.[144]

ICE was formulated based on the belief that threats have now become global and even more dangerous, therefore a new technique was needed to secure the American people.[145] As a result, ICE was granted civil and criminal authority in order to protect national security.[146] The creation of CBP in particular consolidated the roles and responsibilities of multiple organizations into one agency.[147] This enabled CBP to develop unified security procedures and ensure compliance in the nation's health, immigration and international trade regulations and laws.[148] Whereas ICE was created in response to the tragic events of 9/11,[149] CBP actually traces its original functions to the U.S. Customs Service, which was established on July 31, 1789.[150] Although CBP replaced the U.S. Customs Service, its commissioner and the majority of the staff, as well as their responsibilities, transitioned to CBP.[151]

In the present case of *Alasaad v. Nielsen*, the defendants are Secretary of DHS Kirstjen Nielsen, Acting Commissioner of CBP Kevin McAleenan, and Acting Director of ICE Thomas Homan.[152] CBP and ICE are listed as defendants along with the DHS because their policies expressly authorize the challenged searches and confiscations the plaintiffs suffered.[153] These policies are controversial and allegedly unconstitutional because they do not require a warrant, probable cause, or even reasonable suspicion to believe that an electronic device may contain contraband.[154] CBP's previous policy, which was initiated in 2009, authorized

---

142 *March 1, 2003: CBP is Born*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/about/history/march-1-2003-cbp-born (last modified Aug. 1, 2016).

143 Frej, *supra* note 141.

144 *Id.*

145 *See Homeland Security Investigations*, U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, https://www.ice.gov/hsi (last visited Apr. 19, 2019).

146 *History*, U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, https://www.ice.gov/history (last visited Apr. 14, 2019).

147 *CBP Through the Years*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/about/history (last visited Arp. 17, 2019).

148 *Id.*

149 *History*, *supra* note 146.

150 *CBP Through the Years*, *supra* note 147.

151 *Id.*

152 Plaintiff's Memorandum in Opposition of Government's Motion to Dismiss at i, Alasaad v. Nielsen, No. 17-cv-11730-DJC (D. Mass. Jan. 28, 2018).

153 *Id.* at 1.

154 *Id.*

agents to search and examine travelers' electronic devices without any reasonable suspicion.[155] The updated 2018 policy intends to differentiate between a "basic" and an "advanced" search.[156] Basic searches involve an agent tapping or manually searching through an electronic device while opening files or applications.[157] However, advanced searches authorize agents to use software or other devices to essentially conduct a forensic examination of the contents of the device.[158] Under the new policy, basic searches are still permissible without any degree of suspicion, but now advanced searches require reasonable suspicion of illegal activity.[159]

One of the plaintiffs in *Alasaad v. Nielsen*, the Electronic Frontier Foundation ("EFF") identified several problems with the new CBP policy.[160] First, the updated rules have a loophole which allows agents to carry out an advanced search in the interest of national security.[161] The broad interpretation of "national security" as well as "articulable factors" will surely lead to unreasonable and arbitrary searches.[162] Second, by only requiring reasonable suspicion for electronic device searches instead of a probable cause warrant as required by the Constitution, means that the updated policy is still unconstitutional.[163] Third, the distinction between "basic" and "advanced" searches is blurred since basic searches can still be intrusive and violate a traveler's privacy, sometimes even more so than an advanced search.[164] While conducting a basic search, agents can gain access to an individual's text messages, contacts, emails, videos, photos, calendars and browsing history.[165] Collectively, this data viewed as a whole may reveal sensitive and private information about the individual's religion, political beliefs, finances, health, sex life, and family.[166]

However, a positive aspect of the updated CBP policy is that it prohibits an

---

155 Sophia Cope & Aaron Mackey, *New CBP Border Device Search Policy Still Permits Unconstitutional Searches*, ELEC. FRONTIER FOUND. (Jan. 8, 2018), https://www.eff.org/deeplinks/2018/01/new-cbp-border-device-search-policy-still-permits-unconstitutional-searches; U.S. CUSTOMS & BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049: BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION 3 (2009).

156 Cope & Mackey, *supra* note 155; U.S. CUSTOMS & BORDER PROT., *supra* note 155.

157 U.S. DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT UPDATE FOR CBP BORDER SEARCHES OF ELECTRONIC DEVICES DHS/CBP/PIA-008(A) 6 (2018); Cope & Mackey, *supra* note 155.

158 U.S. DEP'T OF HOMELAND SECURITY, supra note 157; Cope & Mackey, *supra* note 155.

159 *Id*.

160 U.S. CUSTOMS AND BORDER PROTECTION, *supra* note 155; Cope & Mackey, *supra* note 155.

161 *Id*.

162 *Id*.

163 *Id*.

164 *Id*.

165 *Id*.

166 *Id*.

agent's access to cloud data and content.[167] Agents instead are required to place devices in airplane mode and disable them from connecting to wireless networks.[168]

The preclusion from accessing cloud content was acknowledged by CBP in a letter that was sent in response to questions posed by U.S. Senator, Ron Wyden, U.S. Senator Rand Paul, and other members of the Senate Finance Committee.[169] Senators Wyden and Paul have been at the forefront of introducing legislation making it illegal for border agents to search and seize electronic devices without a warrant or probable cause.[170] The practice of CBP agents forcing citizens to provide passwords and access to social media is especially alarming for privacy advocates.[171] Senator Wyden asked DHS to clarify this controversial practice, a request which Kevin McAleenan, acting commissioner of CBP, responded to in a letter regarding the cloud policy and its revisions.[172] In the letter, McAleenan stated CBP has officially reminded the agents that they can only access data which is physically present on an electronic device.[173] This statement reversed the 2009 CBP policy, which allowed agents to examine any data or information intercepted during a search, including cloud content.[174] McAleenan clarified that agents are authorized to search a device without the consent of the owner and in rare cases without reasonable suspicion or warrant.[175] However, these searches can only include content that is stored and saved directly onto the device, such as photos, videos, text messages and recent calls.[176] McAleenan concluded that while travelers may refuse to provide their password or unlock their device, agents may confiscate the phone.[177] While privacy advocates such as EFF applaud the enhanced privacy considerations in the new CBP policy, there are still concerns, and ICE has utterly failed to issue an equivalent policy.[178]

---

167 *Id*.

168 U.S. CUSTOMS AND BORDER PROTECTION, *supra* note 155; E.D. Cauchi, *Border Patrol Says It's Barred From Searching Cloud Data on Phones*, NBC NEWS (July 12, 2017), https://www.nbcnews.com/news/us-news/border-patrol-says-it-s-barred-searching-cloud-data-phones-n782416.

169 Cauchi, *supra* note 168; Brian Fung, *Travelers just won back a bit of their privacy at the border*, WASH. POST (July 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/07/14/travelers-just-won-back-a-bit-of-their-privacy-at-the-border/?utm_term=.1a2367ca36f0.

170 Cauchi, *supra* note 168; Fung, *supra* note 169.

171 Cauchi, *supra* note 168; Fung, *supra* note 169.

172 Cauchi, *supra* note 168; Fung, *supra* note 169.

173 Fung, *supra* note 169.

174 Cope & Mackey, *supra* note 155.

175 Cauchi, *supra* note 168; Fung, *supra* note 169.

176 Cauchi, *supra* note 168; Fung, *supra* note 169.

177 Cauchi, *supra* note 168.

178 Cope & Mackey, *supra* note 155.

Moreover, ICE agents are not subject to CBP policies and may access cloud data under their own authority.[179]

IV. *ALASAAD V. NIELSEN*: THE COURT'S OPPORTUNITY TO CLARIFY PROTECTION OF FOURTH AMENDMENT RIGHTS AT THE BORDER

A. Complaint

In September 2017, EFF and ACLU filed a lawsuit against the United States, including DHS, CBP, and ICE, on behalf of eleven plaintiffs who had their electronic devices searched at the border without probable cause or a warrant.[180] The amended complaint alleged that CBP and ICE policies violated the Fourth Amendment by allowing agents to search electronic devices without even a reasonable suspicion that the device contained information indicating that an individual had broken customs or immigration laws.[181] The complaint also challenged the confiscation of electronic devices for extended periods of time without probable cause.[182]

The plaintiffs asked the Court to apply the holding of *Riley v. California* to the instant case relating to the border context.[183] In *Riley*, defendant David Leon Riley was pulled over for driving on expired license registration tags.[184] Riley's license was suspended and police had his car impounded.[185] Before impounding Riley's car the police performed an inventory search which allowed them to search for further hidden contraband.[186] The police found two guns in the car and arrested Riley.[187] During the arrest, Riley had his cell phone in his pocket and detectives discovered photographs of him making gang signs which eventually led to police discovering that Riley was involved in a recent gang shooting.[188] Riley moved to suppress the evidence on his phone, including the photo depicting his gang affiliation as an unreasonable search under the Fourth Amendment.[189] The Supreme Court unanimously rejected the government's argument that searching a cell phone is the same as searching physical items.[190]

---

179 *Id*.

180 Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment rights), *supra* note 37, at 2.

181 *Id*.

182 *Id*.

183 *Id*.; Riley v. California, 134 S. Ct. 2473, 2473 (2014).

184 *Riley*, 134 S. Ct. at 2480.

185 *Id*.

186 *Id*.

187 *Id*.

188 *Id*.

189 *Id*.

190 Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth

The Court stated, "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[191] Therefore, the plaintiffs in the instant case argued that ICE and CBP agents must also obtain a warrant based on probable cause before conducting searches of electronic devices at the border.[192]

B. Motion to Dismiss

Three months after plaintiffs filed the complaint with the United States District Court for the District of Massachusetts, the Government responded with a Memorandum in Support of Defendant's Motion to Dismiss.[193] First, the Government's affirmative defense is that plaintiffs lack the necessary Article III standing to proceed with the case and therefore their claims should be dismissed.[194] However, the plaintiffs asserted that they did have standing on the basis they may suffer an impending injury because they still plan to travel internationally and risk subsequent warrantless searches of their electronic devices.[195] The Government argued that this "speculative fear of future harm does not satisfy the constitutional injury requirement."[196] In light of border search statistics provided in the amended complaint, the Government stated that "there is a miniscule chance of any future border search of Plaintiffs' electronic devices."[197]

The Government also rejected the plaintiff's contention that the warrantless searches of electronic devices at the border constituted a Fourth Amendment violation.[198] Although the Government acknowledged that these searches must be reasonable, they cite *United States v. Montoya de Hernandez*[199] to state that

---

Amendment rights), *supra* note 37, at 3.

191 *Id.*

192 *Id.* at 2-3.

193 Government's Memorandum in Support of Defendant's Motion to Dismiss, Alasaad v. Nielsen, No. 17-cv-11730-DJC (D. Mass. Dec. 15, 2017).

194 *Id*. at 8.

195 Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment rights), *supra* note 37, at 37; Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193.

196 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193.

197 Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment rights), *supra* note 37, at 9; Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193.

198 Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment rights), *supra* note 37, at 14; Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193.

199 United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

"the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior."[200] In *Montoya de Hernandez*,[201] customs officers stopped defendant Rosa Elvira Montoya de Hernandez at the Los Angeles Airport under suspicion that she was a drug mule and was smuggling cocaine from Columbia in her alimentary canal.[202] Montoya de Hernandez did not speak or use the bathroom during the extended detainment, and a court order was obtained by officials for an x-ray.[203] At the hospital, a balloon filled with cocaine was found in her rectum, and eventually Hernandez passed 88 additional balloons filled with cocaine.[204] Montoya de Hernandez argued that her detention violated the Fourth Amendment because customs officers did not have reasonable suspicion to believe that she was smuggling drugs.[205] The Supreme Court found that the standard of proof in this case was met by her numerous recent trips from Bogota to Los Angeles or Miami.[206]

The Government provided an array of cases to distinguish between the various standards of proof required for different electronic devices.[207] In *House v. Napolitano*,[208] the same court as the instant case, held that while some searches "require the government to assert some level of suspicion," the search of a laptop computer "does not invade one's dignity and privacy in the same way" as those searches.[209] In addition, the Ninth Circuit held that reasonable suspicion is the standard of proof for a "forensic examination" of an individual's computer.[210] The Government affirmed its argument that only reasonable suspicion is needed at the border in accordance with *United States v. Kolsuz*,[211] where the court found that "the highest protection available for a border search is reasonable suspicion."[212] The Government also refuted the Plaintiffs' claim that device confiscations for extended periods of time were unconstitutional.[213]

---

200 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193; *Montoya de Hernandez*, 473 U.S. at 538.

201 *Montoya de Hernandez*, 473 U.S. at 532-34.

202 *Id*. at 534.

203 *Id*. at 531.

204 *Id*. at 536.

205 *Id*. at 531.

206 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193; *Montoya de Hernandez*, 473 U.S. at 544.

207 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193.

208 House v. Napolitano, No. 11-10852-DJC, 2012 WL 1038816, at *7 (D. Mass. Mar. 28, 2012).

209 *Id.;* Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193, at 17.

210 United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013).

211 United States v. Kolsuz, 185 F.Supp.3d 843, 859 (E.D. Va. 2016).

212 *Id*.

213 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193, at 26-27.

Specifically, the Government cited to *Montoya de Hernandez*,[214] where the Supreme Court held that instead of time limits "common sense and ordinary human experience must govern over rigid criteria."[215]

The Plaintiff argued the Court should extend the Supreme Court precedent established by *Riley v. California*[216] by holding that law enforcement must have probable cause warrants to conduct searches at the border.[217] The Government strongly disagreed with this interpretation and instead argued that *Riley* limited its holding to the search incident to arrest context.[218] In *Riley* the court stated that while "the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone."[219] The Government contended that the border search doctrine allows full searches of electronic devices unlike the search incident to arrest exception.[220] The threat of contraband, such as child pornography and information pertaining to illegal activity such as malware or "export-controlled material," is easily transferred at the border and serves as a threat to national security.[221] Furthermore, the larger storage capacity of electronic devices maintains a greater amount of contraband and harmful data brought in at the border.[222] For these reasons, the Government contended that *Riley* may not be interpreted to overturn or undermine the border search doctrine and is applied strictly to the search incident to arrest exception.[223] However, the Government's argument to preclude *Riley's* application to this case is insufficient given the present technological landscape. The importance of smart phones and other devices to travelers as raised earlier in this comment show a modern trend towards digital liberty. The Government's argument fails because it is an unsupported blanket statement that does not adequately address the constitutional issue at hand.

---

214 United States v. Montoya de Hernandez, 473 U.S. 531, 543 (1985).

215 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193, at 26-27.

216 *See* Riley v. California, 134 S. Ct. 2473, 2493-95 (2014) (holding that law enforcement needs a warrant to search a cell phone absent exigent circumstances).

217 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193, at 26-27

218 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193, at 19.

219 *Riley*, 134 S. Ct. at 2494.

220 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193, at 20.

221 *Id*.

222 *Id*.

223 *Id*.

C. Opposition to Motion to Dismiss

In January 2018, plaintiffs filed a Memorandum in Opposition to the Government's Motion to Dismiss.[224] The memorandum argued against the Government's attempt to discredit plaintiffs' standing and instead reaffirmed the validity of their claims.[225] Article III standing is established when a plaintiff shows: (1) an "injury in fact"; (2) a "causal connection" between the defendant's conduct and the injury; and (3) probability that a favorable decision by the court will "redress" the alleged injury.[226] The memorandum also cited *City of Los Angeles v. Lyons*,[227] to clarify that the plaintiffs in this case are able to show "a sufficient likelihood that [they] will again be wronged in a similar way."[228] To argue that standing cannot be challenged prematurely, plaintiffs refer to *McBride v. Cahoone*,[229] where the court denied a motion to dismiss an injunctive relief claim because of how early in the stage the motion was filed.[230] The memorandum also emphasized that some plaintiffs have already been accosted multiple times at the border, and therefore it is likely they will be stopped and searched again in the future.[231] Furthermore, the plaintiffs plan to continue traveling internationally to visit family and friends, work or vacation.[232] As a result, plaintiffs are more likely than other travelers to be detained and searched again because their past records will alert agents of past searches and will lead to them suffering the whole ordeal again.[233]

The standing argument that plaintiffs presented to the court have several merits. Most importantly, there is an arguable "injury in fact," as the plaintiffs in this case were seized and had their devices searched without even reasonable suspicion, which is in violation of the Fourth Amendment. Further, plaintiffs satisfy the causation element because the policies of CBP and ICE acting under DHS condone the unconstitutional conduct. Additionally, plaintiffs have proven redressability as border patrol agents have stopped some of the plaintiffs several

---

224 Plaintiffs' Memorandum in Opposition to Defendant's Motion to Dismiss at 1, Alasaad v. Nielsen, No. 17-cv-11730-DJC (D. Mass Jan. 26, 2018).

225 *Id*. at 4-6.

226 Lujuan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992).

227 Plaintiffs' Memorandum in Opposition to Defendant's Motion to Dismiss, *supra* note 224, at 5.

228 City of Los Angeles v. Lyons, 461 U.S. 95, 111 (1983).

229 McBride v. Cahoone, 820 F.Supp.2d 623, 633 (E.D. Pa. 2011).

230 Plaintiffs' Memorandum in Opposition to Defendant's Motion to Dismiss, *supra* note 224, at 5; *Cahoone*, 820 F.Supp.2d at 633.

231 Plaintiffs' Memorandum in Opposition to Defendant's Motion to Dismiss, *supra* note 224, at 6.

232 *Id*.

233 *See id.*; *see, e.g.*, Tabbaa v. Chertoff, No. 05-cv-582D, 2005 WL 3531828, at *7 (W.D.N.Y. Dec. 22, 2005) (stating that government databases with information about past stops "could be used to expand, enhance, or lengthen a border investigation").

times and will likely stop these plaintiffs in the future because they are in the system despite no criminal activity being reported during the first seizure at the border. If national security interests are truly at the forefront it would be most efficient to remove people from the list who have already been interrogated and rule them out as potential criminals. Not only are these searches unconstitutional, but also inefficient and actual criminals can slide by detection. The waste of taxpayer's dollars and build-up of animosity by normal innocent travelers most likely do not help security interests at the border.

Plaintiffs rebutted the Government's opposition to their Fourth Amendment argument by stating that the warrant requirement was created for the exact privacy interests present in the instant case.[234] Plaintiff's memorandum elaborated why electronic devices are dissimilar to physical objects because of their "highly personal" nature and "immense storage capacity."[235] The memorandum stressed that if the court was to rule in favor of the Government, the Government will have access to "a virtual warehouse" of people's lives just because they decide to travel overseas.[236] Plaintiffs believed that *Riley*[237] does not extend any exception to the Fourth Amendment's warrant requirement to digital data searches.[238] Instead, *Riley* required a balancing test between an individual's privacy interests and legitimate governmental interests.[239] While the Government continuously cited the goals of customs and immigration enforcement, it did not address the fact that the warrantless search of electronic devices do not advance these goals.

Although Plaintiffs conceded that illegal digital contraband such as child pornography can be transferred via the border, they pointed out that contraband can easily be transported across the Internet.[240] This highlights the outdated philosophy of the Government because they do not take into consideration how different physical contraband is from digital contraband. For example, drug smuggling involves a physical object being moved through the border while child pornography and other digital crimes are primarily conducted online. The Government pointed to the border search exception to justify warrantless searches but Plaintiffs argued that this exception does not extend to electronic

---

234 Plaintiffs' Opposition to Defendants' Motion to Dismiss and for Summary Judgment, and Plaintiffs' Cross-Motion for Partial Summary Judgment at 14, Alasaad v. Nielsen, No. 17-cv-11730-DJC (D. Mass Feb. 2, 2015).

235 *Id.*

236 *Id.*

237 Riley v. California, 134 S. Ct. 2473, 2489-90 (2014).

238 Plaintiffs' Opposition to Defendants' Motion to Dismiss and for Summary Judgment, and Plaintiffs' Cross-Motion for Partial Summary Judgment, *supra* note 234, at 19.

239 *Id*.

240 *Id.* at 19.

devices and instead agents must obtain probable cause or a warrant to search a device.[241] Plaintiffs maintained that even if warrantless searches advance the government's goals of immigration and customs enforcement, the privacy interests that individuals have in their electronic devices outweigh these governmental interests.[242] Finally, Plaintiffs firmly believed that the harm of warrantless searches will increase as the Government's technological capability to search electronic devices becomes even more powerful.[243]

D. Support of Motion to Dismiss

In March 2018, the Government briefly replied in support of its motion to dismiss.[244] The memorandum made it clear that there is no case law supporting the contention that a border search requires probable cause or a warrant.[245] The Government also reaffirmed its position that Plaintiffs do not have adequate standing to proceed.[246] Namely, the Government argued the Plaintiffs lack standing in accordance with the Supreme Court's holding in *Clapper v. Amnesty Int'l USA,*[247] providing that a group of respondents had lacked standing to challenge the Foreign Intelligence Surveillance Act because their alleged injury was not impending and only hypothetical.[248] In *Clapper*, the Court further stated that it is not enough to establish "an objectively reasonable likelihood of future injury, as that standard is inconsistent with our requirement that threatened injury must be certainly impending to constitute injury in fact."[249] The Government disregarded the Plaintiffs' arguments for standing and alleged that because different reasons were provided for standing this is indicative of the lack of standing.[250]

The Government rejected Plaintiff's interpretation of *Riley* in that a warrant is required for electronic device searches at the border.[251] The memorandum pointed to *United States v. Ramos*,[252] where the Court held that the searches

---

241 *Id*. at 15.
242 *Id*. at 20.
243 *Id*. at 23.
244 Government's Memorandum in Support of Defendants' Motion to Dismiss, *supra* note 193, at 1.
245 *Id*. at 8.
246 *Id*. at 11.
247 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).
248 Government's Memorandum in Support of Defendants' Motion to Dismiss, *supra* note 193, at 14.
249 *Clapper*, 133 S. Ct. at 1143.
250 Government's Memorandum in Support of Defendants' Motion to Dismiss, *supra* note 193, at 9-10.
251 *Id*. at 20.
252 *Id*. at 19.

implicated in *Riley* were to be limited only to search incident to arrest.[253] Furthermore, the Government contended that the warrantless border search of an electronic device was consistent with the justifications for the border search exception which is "protecting the country by preventing unwanted goods from crossing the border into the country."[254] According to *Flores-Montano*,[255] the border search doctrine gives the United States "inherent authority to protect, and a paramount interest in protecting, its territorial integrity."[256] While the plaintiffs believed that the privacy interests of individuals outweigh governmental interests, the Government vehemently disagreed and instead stated that the balance of interests pertaining to the search is "struck much more favorably to the Government at the border."[257] For these reasons, the Government asked the United States District Court for the District of Massachusetts to dismiss the Plaintiffs' amended complaint.[258]

E. Motion to Dismiss Denied

On May 9, 2018, the United States District Court for the District of Massachusetts issued a memorandum and order denying the government's motion to dismiss.[259] The Court ruled that the Plaintiffs had standing on two grounds and their claims that the government's conduct violated the Fourth Amendment were sufficient and the case could continue forward to discovery.[260]

The Court agreed that there was standing because plaintiffs could be subject to future searches at the border and have their electronic devices confiscated again especially since this has already happened to four plaintiffs on multiple occasions.[261] The Court also agreed with plaintiff's allegation that because officers are alerted to past searches in a database the plaintiffs are more likely than other travelers to suffer future searches.[262] The Court stated that "even a

---

253 United States v. Ramos, 190 F.Supp.3d 922, 1002 (S.D. Cal. 2016); *see* Riley v. California, 134 S. Ct. 2473, 2484 (2014).

254 United States v. Feiten, No. 15-200631, 2016 WL 894452, at *6 (E.D. Mich. Mar. 9, 2016); Government's Memorandum in Support of Defendants' Motion to Dismiss, *supra* note 193, at 20.

255 United States v. Flores-Montano, 541 U.S. 149, 153 (2004).

256 *Id.*

257 United States v. Montoya de Hernandez, 473 U.S. 531, 540 (1985); Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193, at 16-17.

258 Government's Memorandum in Support of Defendant's Motion to Dismiss, *supra* note 193, at 16-17.

259 Order Denying Defendant's Motion to Dismiss at 23, Alasaad v. Nielsen, No. 17-CV-11730-DJC (D. Mass May 9, 2018).

260 *Id.* at 11, 12, 21.

261 *Id.* at 10-11.

262 *Id.* at 11.

small probability of injury is sufficient," and disregarded the government's argument that plaintiffs lack standing because of the low odds of a future search.[263] The Court also ruled that the plaintiffs had a second ground of standing in seeking the expungement of data that the government had seized from plaintiffs' devices.[264] The Court agreed with plaintiffs that this would cure future harm resulting from past unconstitutional searches of plaintiffs' devices.[265]

The memorandum denying the Government's motion to dismiss analyzed how the Constitution still protects digital privacy at the border in accordance with the holding in *Riley v. California*[266] which requires police officers to obtain a warrant before searching a cell phone under the Fourth Amendment.[267] In reference to digital privacy, the judge stated that "electronic devices implicate privacy interests in a fundamentally different manner than searches of typical containers or even searches of a person."[268] The Court also adopted the *Riley* approach holding that electronic devices have significant privacy factors because of the vast amount of information it contains about the owner.[269] In the *Alasaad* case, one of the most vital privacy interests was the objection by two plaintiffs, who were Muslim women with religious apprehensions about men looking at pictures of them without their traditional hijab.[270] The *Alasaad* court also recognized how manual searches are as intrusive as a forensic search.[271] A "forensic" search is when the officer must use their own digital device to search the travelers' device, whereas a "manual" search allows the officer to take advantage of each travelers' device and search its contents.[272] Additionally, the Court provided that a manual search renders the same quantity and quality of information aa a forensic search, and therefore there is no difference in the level of privacy invasion from these searches.[273]

In analyzing the government's interests, the judge again looked to *Riley* to clarify that any warrantless search of effects such as electronic devices must be "tethered" to the government's interests.[274] The government's interests at the border in conducting warrantless searches are mainly to prevent the entry of

---

263 *Id*.
264 Order Denying Defendant's Motion to Dismiss, *supra* note 259, at 12.
265 *Id*. at 12.
266 *Id*. at 20; Riley v. California, 134 S. Ct. 2473, 2485 (2014).
267 *Riley*, 134 S. Ct. at 2485, 2493.
268 Order Denying Defendant's Motion to Dismiss, *supra* note 259, at 19.
269 *Id*. at 15; *Riley*, 134 S. Ct. at 2489.
270 Complaint for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment rights), *supra* note 37, at 18.
271 Order Denying Defendant's Motion to Dismiss, *supra* note 259, at 2.
272 *Id*. at 2.
273 *Id*. at 14.
274 *Id*. at 18-19; *see* Riley v. California, 134 S. Ct. 2473, 2485, 2494 (2014).

harmful items and contraband.[275] The question the Court proffers is whether the warrantless searches of devices advance these interests.[276] The judge agreed with the Plaintiffs that there is a significant contrast between searching for contraband and searching for evidence of unlawful activity, with the latter having a weaker tethering.[277] The court also ruled that a warrant requirement would not negatively impact the government's interests at the border and with the new technology the process of securing a warrant would be more efficient.[278] Specifically, the judge stated that "it is unclear at this juncture the extent to which a warrant requirement would impede customs officers' ability to ferret out such contraband."[279] The Court disagreed with Government's unsupported claim that child pornography vindicates the warrantless searches of devices at the border.[280] In accordance with *Riley*, the Court stated that the Government must show that the issue they intend to solve with warrantless searches is "prevalent."[281] Government data has shown that the majority of child pornography is accessed on the Internet instead of being brought over the border.[282]

The Court also stated that the plaintiffs credibly alleged that the lengthy confiscations of devices without a warrant violated the Fourth Amendment.[283] In the opinion the judge held that seizures must "be reasonable not only at their inception but also for their duration."[284] The Court looked specifically at the cases of Mr. Allababidi who had his device confiscated for ten months and Mr. Wright whose device was confiscated for fifty-six days.[285]

Although the Court's opinion was a huge victory for the plaintiffs in the *Alasaad* case, the issue remains regarding what level of individualized suspicion a border agent must have before seizing and searching an electronic device.[286] Throughout the case the Government has asserted that the lowest level of protection, reasonable suspicion is required while the plaintiffs demand the highest level of protection, which deems a warrant.[287] Although this question

---

275 United States v. Montoya De Hernandez, 473 U.S. 531, 532 (1985).
276 Order Denying Defendant's Motion to Dismiss, *supra* note 259, at 18-19.
277 *Id*. at 18.
278 *Id*. at 19.
279 *Id*.
280 *Id*.
281 *Id*.; *see* Riley v. California, 134 S. Ct. 2473, 2485 (2014).
282 Order Denying Defendant's Motion to Dismiss, *supra* note 259, at 19; U.S. SENT'G COMMISSION, FEDERAL CHILD PORNOGRAPHY OFFENSES 41-42 (2012).
283 Order Denying Defendant's Motion to Dismiss, *supra* note 259, at 21.
284 *Id*. at 21.
285 *Id*.
286 *Id*. at 17.
287 *Id*.

was not answered by the court the judge advised that a warrant might be the best choice because with a reasonable suspicion standard there would be "no practical limit at all."[288]

F. Government Shutdown

On January 2, 2019, the Government asked the *Alasaad* court to freeze discovery in the case, claiming that its lawyers cannot perform any work due to the government shutdown that occurred on December 21, 2018.[289] The lapse of funding has prevented the defendants—DHS, CBP and ICE—from gathering the necessary documents for discovery.[290] The shutdown is a result of President Trump's demand for $5 billion dollars to build a wall along the U.S.-Mexico border.[291] Discovery deadlines were spread throughout the month of January—the government owed discovery responses by January 8, 2019, both sides planned to conduct depositions the week of January 14, 2019 and the final deadline for discovery was set for January 31, 2019.[292] The ACLU and EFF have not responded to any requests for a comment about freezing discovery but according to court records plaintiffs have taken no position on the motion for a stay, but instead reserve the right to ask the court to lift it.[293]

V. RANDOM PROFILING OR DISCRIMINATION?

The CBP has stated that it is their policy not to consider race or ethnicity when it comes to investigation, screening and law enforcement.[294] The DHS has also issued a policy outlining nondiscriminatory screening and law enforcement activities.[295] The DHS defines "racial profiling" as the "invidious use of race or ethnicity as a criterion."[296] The DHS also notes that "racial profiling is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual

---

288 *Id*. at 15.

289 Aaron Leibowitz, *Feds Request Pause In Border Search Case Due To Shutdown*, Law360 (Jan. 2, 2019) https://www-law360-com.cualaw.idm.oclc.org/articles/1114694/feds-request-pause-in-border-search-case-due-to-shutdown.

290 *Id*.

291 *Id*.

292 *Id*.

293 *Id*.

294 *CBP Policy on Nondiscrimination in Law Enforcement Activities and all other Administered Programs*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/about/eeo-diversity/policies/nondiscrimination-law-enforcement-activities-and-all-other-administered (last modified Aug. 10, 2017).

295 *Id*.

296 *Id*.

of another race or ethnicity."[297] However, CBP personnel are allowed to use ethnicity or race whenever a "compelling governmental interest is present and its use is narrowly tailored to that interest."[298] The CBP further states that "national security is per se a compelling interest."[299] At a time when the current administration has campaigned on a nationalist approach and is constantly in battle with Congress to restrict immigration,[300] it is hard to reconcile that race or ethnicity had nothing to do with the Plaintiffs detainment in the instant case of *Alasaad v. Nielsen*.[301]

The Alasaad family are the key plaintiffs in this case.[302] Despite the fact that Ghassan and Nadia Alasaad are both U.S. citizens, CBP agents humiliated them without probable cause, nor reasonable suspicion, and without regard that they were traveling with their sick 11-year old daughter.[303] When Nadia objected to providing the password for her phone because of photos of herself without her hijab, the CBP officer told the family that if a password was not provided Nadia's phone would be confiscated.[304] Along with Nadia and Ghassan there are nine other plaintiffs in the instant case with different occupations and backgrounds, all of whom have had similar experiences when crossing the border.[305]

Suhaib Allababidi is an entrepreneur from Texas who owns a security installation system with clients in the Federal Government.[306] Two phones were confiscated from him and returned two months later.[307] Another plaintiff, Sidd Bikkannavar, is an engineer from California who works in NASA's Jet Propulsion Laboratory.[308] Bikkannavar's work phone was searched with forensic tools and his private information was analyzed.[309] Plaintiff Jeremy Dupin, who was detained two days in a row while traveling proves that journalists and filmmakers are not safe either.[310] Dupin's phone was unlocked forcefully and his sensitive journalism research was inspected.[311] CBP even

---

297 *Id*.
298 *Id*.
299 *Id*.
300 Hatmaker, *supra* note 67.
301 *Id*.
302 *See* Compliant for Injunctive and Declaratory Relief (Violation of First and Fourth Amendment rights), *supra* note 37.
303 *Id*. at 5, 17.
304 *Id*. at 17-18.
305 ELEC. FRONTIER FOUND., *supra* note 1.
306 *Id*.
307 *Id*.
308 *Id*.
309 *Id*.
310 *Id*.
311 *Id*.

detained professor and artist, Aaron Gach, who was detained until he provided his phone's password to agents.[312] Another journalist, Isma'il Kushkush from Virginia was detained three different times and had his phone searched for hours each time.[313] One of the most shocking plaintiffs who was detained by CBP was Diane Maye, a former Air Force captain and current professor who was subjected to a two hour search of her laptop and phone.[314] Another plaintiff with impressive credentials, Zainab Merchant, a graduate student at Harvard University had her laptop and phone searched for two hours as well.[315] Unfortunately, CBP has even become physical with plaintiffs such as Akram Shibly, an independent filmmaker from New York who was detained twice in a period of days and had his phone searched after agents physically restrained him.[316] The final plaintiff included in the instant case is Matt Wright, an independent computer programmer from Colorado who had his laptop, smart phone and camera confiscated for two months.[317]

The EFF has addressed that several of the Plaintiffs are Muslims and people of color who have been singled out by CBP agents "newly emboldened by this administration's aggressive pursuit of travel and immigration policies targeting those groups."[318] Plaintiffs argue that the stereotyping of Muslims proves that CBP and ICE officers do not have reasonable suspicion to search devices but instead are carrying out searches based on a traveler's background or religion. The current political landscape in the United States indicates that there is a racist and discriminatory view of Muslims by members of the current administration.

For instance, in January 2018, Trump claimed "I'm not a racist. I am the least racist person you have ever interviewed, that I can tell you," in response to comments he was reported to have made, which included a derogatory reference made regarding African nations.[319] Trump even started off his campaign with an infamous speech and example of harmful stereotyping and generalizing about Mexicans stating, "They're bringing drugs. They're bringing crime. They're rapists. And some, I assume, are good people."[320] There are numerous well-

---

312 Matt Cagle & Chris Conley, *Why Did the Government Search an Artist's iPhone at the Border?*, ACLU (May 4, 2017), https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/why-did-government-search-artists-iphone.

313 ELEC. FRONTIER FOUND., *supra* note 1.

314 *Id.*

315 *Id.*

316 *Id.*

317 *Id.*

318 Hatmaker, *supra* note 67.

319 Michael D. Shear, *'I'm Not a Racist,' Trump Says in Denying Vulgar Comment*, N.Y. TIMES (Jan. 14, 2018), https://www.nytimes.com/2018/01/14/us/politics/trump-im-not-a-racist.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news.

320 Alexander Burns, *Choice Words From Donald Trump, Presidential Candidate*, N.Y.

documented incidents of Trump's racism spanning back in time since his days as a real estate developer in the 1970's and 1980's.[321] Although there is a vast amount of information highlighting Trump's racist behavior for the purpose of this comment only statements and conduct towards Muslims will be analyzed and an argument will be made that his behavior and attitude towards Muslims has indirectly caused the racial stereotyping and discriminating against Muslim travelers by CBP and ICE officials.

In December 2015, Trump called for a "total and complete shutdown" of the entry of Muslims to the United States "until our country's representatives can figure out what is going on."[322] Along with this statement released by his campaign, Trump included poll data that allegedly showed that a large group of the Muslim population has "great hatred towards Americans."[323] In July 2016, Trump disparaged the parents of a slain Muslim soldier who had received a gold star during his service. Trump speculated that only the soldier's father spoke at the Democratic National Convention, and not the mother because "maybe she wasn't allowed to have anything to say."[324] Trump's comment that the soldier's mother could not speak at the convention because of the obedience expected of traditional Islamic women, is another classic example of stereotyping Muslims.[325]

Lastly, in January 2017, Trump's racism towards Muslims was embodied with his creation and execution of what has been referred to as the "Muslim Ban" or "Executive Order 13769, Protecting the Nation from Foreign Terrorist Entry into the United States" which are a series of discriminatory executive orders issued by Trump.[326] The first version, which was signed by Trump and enacted the same day, was immediately blocked by federal courts, which found it to be unconstitutional, anti-Muslim, and a blatant abuse of the President's power.[327]

TIMES (June 16, 2015, 2:01 PM), https://www.nytimes.com/politics/first-draft/2015/06/16/choice-words-from-donald-trump-presidential-candidate.

321 David Leonhardt & Ian Prasad Philbrick, *Donald Trump's Racism: The Definitive List*, N.Y. TIMES (Jan. 15, 2018), https://www.nytimes.com/interactive/2018/01/15/opinion/leonhardt-trump-racist.html.

322 Jenna Johnson, *Trump calls for 'total and complete shutdown of Muslims entering the United States'*, WASH. POST (Dec. 7, 2015, 7:43 PM), https://www.washingtonpost.com/news/post-politics/wp/2015/12/07/donald-trump-calls-for-total-and-complete-shutdown-of-muslims-entering-the-united-states/?noredirect=on&utm_term=.b6bb461fc276.

323 *Id*.

324 Maggie Haberman & Richard A. Oppel Jr., *Ire for Trump as He Derides Muslim Parents*, N.Y. TIMES, July 31, 2016, at 1.

325 *Id*.

326 Subha Varadarajan, *Understanding Trump's Muslim Bans*, NAT'L IMMIGR. L CTR. (Sept. 11, 2018), https://www.nilc.org/issues/immigration-enforcement/understanding-the-muslim-bans.

327 *Id*.

Although a majority of the public agree, the U.S. Supreme Court, allowed the latest version of the ban to go into effect.[328] According to Wired Magazine, "since President Trump's executive order [Muslim ban] ratcheted up the vetting of travelers from majority Muslim countries, or even people with Muslim-sounding names, passengers have experienced what appears from limited data to be a 'spike' in cases of their devices being seized."[329]

A. Unlawful Searches by CBP and ICE of Specific Racial and Religious Groups Violates the Equal Protection and Due Process Clauses of the Constitution

The 5th Amendment of the United States Constitution states:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.[330]

The Equal Protection Clause in the amendment states that no person can be deprived of life, liberty, or property without due process.[331] Due process requires that all legal proceedings will be fair and reasonable.[332] The Equal Protection Clause of the Fourteenth Amendment applies to the federal government through the Due Process Clause of the Fifth Amendment.[333] The Equal Protection Clause of the Fourteenth Amendment prevents the government from discriminating on the basis of religion, race, religion, and national origin.[334] Therefore, border agents are not allowed to target travelers because they are Muslim in order to search and seize their electronic devices at the border.[335] At one point the Supreme Court in *United States v. Brignoni-Ponce* [336] suggested that agents operating at the Mexican border may look at a traveler's origin in order to

---

328 *Id*.
329 Greenberg, *supra* note 62.
330 U.S. CONST. amend. V.
331 *Id*.
332 *Id*.
333 SOPHIA COPE ET AL., DIGITAL PRIVACY AT THE U.S BORDER: PROTECTING THE DATA ON YOUR DEVICES AND IN THE CLOUD 32 (2017).
334 U.S. CONST. amend. XIV, § 1.
335 COPE ET AL., *supra* note 333.
336 United States v. Brignoni-Ponce, 422 U.S. 873, 886-87 (1975).

establish reasonable suspicion of an immigration violation.[337] However in *United States v. Montero-Camargo*, [338] a U.S. Circuit Court determined that this suggestion is not considered anymore due to the changes in demographics and constitutional law.[339] The operation of policies which were enacted under Trump's administration unfairly discriminates against Muslims in violation of the Fifth and Fourteenth Amendment.

VI: GETTING PAST CUSTOMS WITH ONE'S DIGITAL PRIVACY INTACT

Instead of arguing or agreeing with CBP or ICE agents, technological experts advise travelers to avoid making themselves a victim of arbitrary searches of devices.[340] Wired magazine has provided tips and advice for travelers who want to keep their digital privacy intact and not be arrested as a result.[341] Locking your device is recommended and travelers can even encrypt their hard drive "with tools like BitLocker, TrueCrypt, or Apple's Filevault, and choose a strong passphrase."[342] Remembering to turn off devices before entering customs is another solution.[343] If you own an iPhone, activating TouchID will require a PIN rather than one's fingerprint when the phone is turned on.[344] This option resolves the issue of border agents compelling you to unlock your device with a finger especially since green card holders must provide fingerprints at every border.[345] Keeping passwords a secret from CBP agents is another complex issue.[346] Although United States citizens may refuse to provide their passwords, such citizens risk prolonged detainment and confiscation of their electronic device.[347] However, by refusing to reveal the PIN or password to your device, travelers will likely be able to cross the border with their digital privacy intact.[348] Travelers should also be in communication with a lawyer, or someone who can assist them in contacting legal counsel.[349] It is recommended that before entering

---

337 *See id*.
338 United States v. Montero-Camargo, 208 F.3d 1122, 1131-35 (9th Cir. 2000) (en banc).
339 *Id*.
340 *See* Greenberg, *supra* note 62.
341 *Id*.
342 *Id*.
343 *Id*.
344 *Id*.
345 Stephanie Condon, *DHS wants green card holders' fingerprints*, CNET (Dec. 18, 2008, 8:16 PM), https://www.cnet.com/news/dhs-wants-green-card-holders-fingerprints/.
346 Greenberg, *supra* note 62.
347 *Id*.
348 *Id*.
349 *Id*.

customs inspection the traveler should contact a third party and then again once they pass through customs.[350] In the event that you are detained or interrogated at least then there is someone on the outside who can help.[351]

Denying yourself access is an extreme option which involves bold but easy steps.[352] First, create a "two-factor authentication"[353] for private accounts, so that in order to access them you need a password as well as a code, which has been sent to your phone in the form of a text message.[354] Second, before crossing the border leave behind the SIM card which will receive the text message code.[355] This method "essentially den[ies] yourself the ability to cooperate with agents even if you wanted to."[356] Overall, the best advice for travelers who are at risk of device searches is to pack it in your checked bag or suitcase.[357] This will protect their digital privacy and people always have the option to carry a designated travel phone with no sensitive data.[358]

VII. CONCLUSION

In the case of *Alasaad v. Nielsen*, it is this comment's opinion that the United States District Court of Massachusetts should find the Governments' warrantless searches of travelers' electronic devices a violation of the Fourth Amendment. Agents should have probable cause and a warrant to seize and search a traveler's device for contraband or evidence of activity in violation of customs and immigration laws. Currently, agents do not have to show individualized and particularized suspicion for any specific device which makes their authority arbitrary and unreasonable. Plaintiffs should be granted declaratory and injunctive relief against these unlawful searches and seizures. In the near future, CBP and ICE policies should be further inspected and transformed with digital privacy being taken into account, as well as devoid of any stereotyping and discriminatory actions towards Muslim travelers.

---

350 Cory Doctorow, *How to legally cross a US (or other) border without surrendering your data and passwords*, BOING BOING (Feb. 12, 2017, 7:44 AM), https://boingboing.net/2017/02/12/how-to-cross-a-us-or-other-b.html.

351 *Id*.

352 Greenberg, *supra* note 62.

353 *Id*.

354 *Id*.

355 *Id*.

356 *Id*.

357 *See id*. (explaining how "for the most vulnerable travelers, the best way to keep customs away from [their] data is simply not to carry it").

358 *See* Russell Brandom, *Want to protect your data at the border? Delete it*, THE VERGE (Feb. 15, 2017, 3:57 PM), https://www.theverge.com/2017/2/15/14629022/border-search-customs-data-privacy-encryption.