The First Circuit's Incorrect Ruling in *Alasaad v. Mayorkas*: How the Fourth Amendment's Border Search Exception Should Apply to Electronic Devices

Joana Jankulla[*]

INTRODUCTION

As it currently stands in the First Circuit, individuals traveling through the United States' borders may have their electronic devices searched at any time.[1] The Fourth Amendment protects all individuals from unreasonable searches and seizures, meaning probable cause and a warrant are generally required before conducting a search or seizure.[2] However, numerous exceptions to the Fourth Amendment exist; among them is the border search exception.[3] Under this exception, border patrol officers are given full authority to conduct basic searches of individuals and items crossing the border.[4] However, controversy has emerged regarding electronic devices at the border, as many believe they should not fall within this exception and a level

[*] J.D., New England Law | Boston (2023). B.A., Classical Studies with high honors & Language and Linguistics, Brandeis University (2018). I would like to thank my editors, Madison Piotrowski and Ciaran O'Dwyer, for their assistance in helping me craft this case comment. I would also like to the entire *New England Law Review* v. 56 and v.57 staff for all they do. Finally, I would like to thank Ian for always inspiring me to keep going.

[1] *See Recent Cases: Fourth Amendment — Border Search Exception — First Circuit Upholds Warrantless, Suspicionless Searches of Electronic Devices at The Border* — Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021), 135 HARV. L. REV. 1464, 1464 (2022), https://perma.cc/N6FQ-J969 [hereinafter *Recent Cases*].

[2] *See* HILLEL R. SMITH, KELSEY Y. SANTAMARIA & CONG. RSCH. SERV., R46601: SEARCHES AND SEIZURES AT THE BORDER AND THE FOURTH AMENDMENT 12 (2021), https://perma.cc/YS6A-6PYY [hereinafter SMITH ET AL.].

[3] *Id.* at 25.

[4] *See id.* at 3–4.

of suspicion should be required before searching a person's device.[5]

In *Alasaad v. Mayorkas*, the First Circuit established its stance within this controversy, which many circuit courts have wrestled with.[6] Prior to *Alasaad*, the scope of basic and advanced searches of electronic devices allowed at the border was not clear in the First Circuit.[7] The First Circuit ruled in favor of the governmental authority, stating that basic searches require no level of suspicion while advanced searches require only minimal suspicion to search for both contraband and evidence of contraband.[8] The plaintiffs in *Alasaad* filed a writ of certiorari on April 23, 2021.[9] On June 28, 2021, the Supreme Court denied this petition and to this day there is no precedent set by the Supreme Court on how electronic devices should be handled at the border.[10]

This Comment will illustrate that the holding in *Alasaad v. Mayorkas* should be overruled, since although the interest of the government is at its "zenith" at the border, this ruling infringes on the individual privacy interests afforded by the Fourth Amendment. Part I discusses how the Fourth Amendment evolved over time to include certain warrant exceptions. Part II discusses the facts, procedural history, and First Circuit holding and analysis in *Alasaad v. Mayorkas.* Part III will argue that basic searches of electronic devices at the border should require reasonable suspicion; although the government has a heightened interest in preventing contraband from entering the country, the Fourth Amendment still requires the government to uphold basic privacy rights of individuals. Part IV will argue that the scope of advanced searches should not include searching for evidence of contraband, as the parameters of such a search are not well-defined and therefore allow for a potential abuse of power by border patrol agents.

I. Background

A. *Fourth Amendment Searches and Seizures*

The Fourth Amendment of the United States Constitution gives individuals the right to security in their "persons, houses, papers, and

---

[5] *See generally id.* at 45–48 (explaining the nature of the border-search exception with electronic devices).

[6] 988 F.3d 8, 12–13 (1st Cir. 2021).

[7] *See generally id.* at 13.

[8] *See id.* at 18–19.

[9] *Merchant v. Mayorkas*, SCOTUSBLOG, https://perma.cc/MLS2-FKLB (last visited Apr. 25, 2023).

[10] *See id.*

effects, against unreasonable searches and seizures . . . ."[11] A Fourth Amendment search occurs when an individual's reasonable expectation of privacy is infringed.[12] A Fourth Amendment seizure of a person occurs when police conduct would communicate to a reasonable person, taking the circumstances into account, that they are not free to ignore police presence and leave at their own will.[13] A Fourth Amendment seizure of property occurs when an individual's possessory interest in that property is in some way inhibited.[14] Additionally, the Fourth Amendment lists the parameters for obtaining a warrant: the requirements of probable cause and a description of what the search will entail.[15] Finally, a warrant is finalized upon approval by a judge or magistrate.[16]

In *Carroll v. U.S.*, the Court stated that probable cause "aris[es] out of circumstances known to the seizing officer," that contraband or evidence of a crime will be found in the vehicle to be searched.[17] The standard for probable cause to arrest is described as "whether, at the moment the arrest was made, the officers . . . had reasonably trustworthy information . . . sufficient to warrant a prudent man in believing that the petitioner had committed or was committing an offense."[18] The Supreme Court stated that individuals have the right both to their possessions and to control of themselves against unlawful, unreasonable restraint.[19] It is important to note that the root of the Fourth Amendment requires evaluating how reasonable a search is.[20]

In *Katz v. United States*, the defendant was convicted for sending wagering information via telephone.[21] During his trial, the government brought in evidence that FBI agents placed a listening and recording device outside the public phone booth the defendant walked into to make phone

---

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

[12] Soldal v. Cook County, Ill., 506 U.S. 56, 63 (1992).

[13] *See* Terry v. Ohio, 392 U.S. 1, 16–17 (1968).

[14] *See Soldal*, 506 U.S. at 61.

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

[16] Katz v. United States, 389 U.S. 347, 357 (1967).

[17] 267 U.S. 132, 149 (1925).

[18] Beck v. Ohio, 379 U.S. 89, 91 (1964).

[19] Terry v. Ohio, 392 U.S. 1, 9 (1968).

[20] *See* SMITH ET AL., *supra* note 2, at 1.

[21] 389 U.S. at 348.

calls.[22] In a landmark decision, the Supreme Court stated that the government violated the privacy of the defendant when agents listened in on his call.[23] This conduct was a search and violated the Fourth Amendment because of (1) use of the recording device prior to establishing probable cause and (2) lack of a warrant.[24] Justice Harlan articulated a reasonable expectation of privacy test in his concurring opinion.[25] This test has two prongs: first, "a person [must] have exhibited an actual (subjective) expectation of privacy"; and second, "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[26] Justice Harlan noted that "one who occupies [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call" is may reasonably think that his conversation is truly private and not being intercepted.[27] The government argued that Katz did not have a privacy right in the phone booth, because it was made of glass, and he was visible to the public.[28] However, Katz did not lose his reasonable expectation of privacy just because he "made his calls from a place where he might be seen" as the concern did not come from the "intruding eye" but rather the "uninvited ear" meaning he intended to prevent the outside world from hearing his conversation inside the phone booth.[29]

B. *Fourth Amendment Exceptions*

In general, the Fourth Amendment requires the establishment of probable cause before issuing a warrant for a search or seizure, but exceptions to this rule exist.[30] Among them are the Terry stop exception, the search incident to arrest exception, and the border search exception.[31] These exceptions make it possible to conduct a search or seizure without a warrant.[32]

---

[22] *Id.*

[23] *Id.* at 353.

[24] *Id.*

[25] *Id.* at 360 (Harlan, J., concurring).

[26] *Id.* at 361 (Harlan, J., concurring).

[27] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[28] *Id.* at 352.

[29] *Id.*

[30] *See* Terry v. Ohio, 392 U.S. 1, 11 (1968).

[31] *See* SMITH ET AL., *supra* note 2, at 1–2.

[32] *See* SMITH ET AL., *supra* note 2, at 1–2.

1. The "Terry Stop" Exception

In *Terry v. Ohio*, Terry experienced a pat down by a police officer who suspected he intended to commit a robbery.[33] Ultimately, the officer did not need probable cause; to determine the reasonableness and validity of the search the Court balanced the government's interest with the intrusion of privacy as a whole.[34] The officer must "point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[35] The court determined that a pat down—a limited search of the outside of a person's clothing—is reasonable if an officer can point to unusual conduct that leads him to suspect criminal activity, as the officer is entitled to protect not just himself but the public.[36] The Terry stop exception demonstrates a standard less than probable cause known as "reasonable suspicion."[37] This allows the police officer "to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons which might be used to assault him."[38] This search is a reasonable search under the Fourth Amendment.[39]

2. The Search Incident to Arrest Exception

In *U.S. v. Robinson*, an officer pulled over the defendant, conducted a pat down, and found heroin in his pocket.[40] The Supreme Court ruled this a valid Fourth Amendment search as it remained within the scope of the search incident to arrest exception.[41] Under this exception, a search is reasonable if it is preceded by an arrest, based on the need to protect the public and discover potential evidence regardless of whether such evidence is found.[42]

In *Riley v. California*, after Riley's arrest police officers searched his phone

---

[33] 392 U.S. at 6–7.

[34] Shan Patel, Note, *Per Se Reasonable Suspicion: Police Authority to Stop Those Who Flee from Road Checkpoints*, 56 DUKE L.J. 1621, 1625 (2007).

[35] *Terry*, 392 U.S. at 21.

[36] *Id.* at 24.

[37] *See* Patel, *supra* note 34, at 1625.

[38] *Terry*, 392 U.S. at 30.

[39] *Id.* at 31.

[40] 414 U.S. 218, 222–23 (1973).

[41] *Id.* at 235.

[42] *See id.* at 235–36.

and found evidence which connected him to an earlier crime.[43] The Supreme Court held that in this instance the officers first needed a warrant to search Riley's phone as "[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."[44] An officer can inspect the physical contents of a cell phone to ensure it is not a weapon.[45] However, a warrant is required before conducting an internal search of the cell phone.[46]

3. The Border Search Exception

The basis of the border search requirement emerged in 1789 when Congress enacted a statute that gave officials at the border the power to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed."[47] This exception to the Fourth Amendment applies to any U.S. border which is based on the government's heightened interest in stopping contraband from entering the country.[48]

The Supreme Court addressed the issue of border searches in many notable cases.[49] In *United States v. Flores-Montano*, the Court proclaimed: "[t]he government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[50] Here, the government disassembled and searched a car's fuel tank.[51] The Court concluded that the government's significant interest at the border allows it to have authority to conduct searches with no level of suspicion.[52] In *U.S. v. Montoya de Hernandez*, the Court noted that the reasonable suspicion needed to detain a traveler at the border, beyond a routine search, is a balance between private and public interests, and is valid if the facts in those

---

[43] 573 U.S. 373, 373 (2014).

[44] *Id.* at 386–87.

[45] *Id.*

[46] *Id.*

[47] Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1105 (2009).

[48] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

[49] *See generally* Ashley Veronica Hart, Note, *Electronic Searches at the Border: Reasonable Suspicion or None at All? The Circuit Split and Potential Impact on Higher Education*, 54 SUFFOLK U. L. REV. 371, 377–78 (2021) (explaining the instances in which the issue of border searches was addressed by the Supreme Court).

[50] 541 U.S. 149, 152 (2004).

[51] *Id.* at 150–51.

[52] *See id.* at 155–56.

circumstances make officials suspect the existence of contraband.[53]

Many circuit courts have addressed the issue of border searches of electronic devices.[54] The Fifth Circuit permitted a warrantless search of an electronic device at the border.[55] The Fourth Circuit required at least reasonable suspicion to conduct warrantless border searches of electronic devices.[56] The Ninth Circuit required reasonable suspicion for advanced searches of electronic devices at the border.[57] Six years later, the Ninth Circuit added to this by arguing that while the border-search exception allows for the warrantless search of a cell phone, it only applies to searching for contraband, not evidence of contraband.[58]

C. *The Authority of Immigration Agencies at the Border*

The Immigration and Nationality Act ("INA") authorizes immigration officers to conduct searches and seizures at the border.[59] The Department of Homeland Security ("DHS") is an agency whose main obligation is to implement immigration laws.[60] DHS works with Customs and Border Protection ("CBP") as well as Immigration and Customs Enforcement ("ICE") to enforce these laws at the border.[61]

CBP Directive No. 3340-049A on border searches of electronic devices provides "guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in . . . mobile phones . . . and any other communication, electronic, or digital devices . . . to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer."[62] This CBP policy defines an electronic device as "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other

---

[53] *See* 473 U.S. at 541.

[54] *See* Hart, *supra* note 49, at 388–89.

[55] United States v. Molina-Isidoro, 884 F.3d 287, 293 (5th Cir. 2018).

[56] United States v. Kolsuz, 890 F.3d 133, 148 (4th Cir. 2018).

[57] United States v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013).

[58] United States v. Cano, 934 F.3d 1002, 1021 (9th Cir. 2019).

[59] SMITH ET AL., *supra* note 2, at 8.

[60] SMITH ET AL., *supra* note 2, at 7.

[61] SMITH ET AL., *supra* note 2, at 7–8.

[62] Border Search of Electronic Devices, Directive No. 3340-049A 1 (CBP Jan. 4, 2018), https://perma.cc/VKS8-ALT9.

media players."[63] According to CBP, a basic search is any non-advanced search performed without reasonable suspicion.[64] An advanced search is "any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."[65] Further, advanced searches require supervisory approval and can only be performed in instances "in which there is reasonable suspicion of activity in violation of the laws enforced or administered by the CBP, or in which there is a national security concern . . . ."[66]

ICE Directive No. 7-6.1 describes ICE policy on searches of electronic devices at the border and is meant to provide guidelines that ICE must follow.[67] ICE defines an electronic device as "[a]ny item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices."[68] ICE policy states that while basic searches do not require suspicion, advanced searches require only a level of reasonable suspicion.[69] Additionally, agents can keep electronic devices for a "reasonable time given the facts and circumstances of the particular search."[70] Although both CBP and ICE policies define different types of searches, it is unclear where the line is drawn between a basic and an advanced search.[71]

II. The Court's Opinion

A. *Factual History*

A group of plaintiffs filed an initial suit in the District Court of Massachusetts and alleged a violation of their First and Fourth Amendment rights when border patrol agents searched their electronic devices.[72] Agents searched each plaintiff's electronic device at least once, which included

---

[63] *Id.* at 2.

[64] *See id.* at 4.

[65] *Id.* at 5.

[66] *Id.*

[67] Border Searches of Electronic Devices, Directive No. 7-6.1 1 (ICE Aug. 18, 2009), https://perma.cc/9XXK-W7PE.

[68] *Id.* at 2.

[69] *See* Alasaad v. Nielsen, 419 F. Supp. 3d 142, 148 (D. Mass. 2019).

[70] Border Searches of Electronic Devices, Directive No. 7-6.1 4 (ICE Aug. 18, 2009), https://perma.cc/9XXK-W7PE.

[71] *See* SMITH ET AL., *supra* note 2, at 21.

[72] Alasaad v. Mayorkas, 988 F.3d 8, 12–13 (1st Cir. 2021).

smartphones and laptops, and agents searched the electronic devices of five plaintiffs multiple times.[73] CBP officers searched Nadia Alasaad's, the namesake of this lawsuit, electronic devices twice, and these officers did not respect her religious beliefs by ignoring her request to stop looking at photos on her phone that contained images of Alasaad and her daughters without their headscarves on.[74] Alasaad noted that a CBP officer noticed a photo on her phone the first time they searched it but did not notice this photo on her phone during the second search.[75] Merchant, a plaintiff and owner of a media website, also experienced multiple searches of her electronic devices.[76] Officers not only noticed photos of Merchant without her headscarf on, but read privileged attorney-client communications on her phone.[77] Another plaintiff, a journalist, stored information regarding his work on his phone.[78] Yet another plaintiff's phone, owned by his employer NASA, contained confidential information.[79] CBP officers not only conducted searches of the electronic devices, but also made additional "observations or characterizations of the information contained therein," such as lack of contraband or the contents of a social media post.[80] One plaintiff noted that CBP "extracted and retained" information from his electronic devices and kept his devices for fifty-six days.[81]

B. *The Court's Holding*

The District Court held that basic and advanced border searches of electronic devices required reasonable suspicion.[82] The First Circuit agreed with the Ninth and Eleventh Circuits and ruled that routine searches at the border did not need any level of suspicion.[83] They stated that the ruling in *Riley* did not apply to the border, as the search of an electronic device is

---

[73] *Nielsen*, 419 F. Supp. 3d at 149.

[74] *Id.* at 149.

[75] *Id.*

[76] *Id.* at 149–50.

[77] *Id.*

[78] Alasaad v. Nielsen, 419 F. Supp. 3d 142, 150 (D. Mass. 2019).

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.* at 165–68.

[83] Alasaad v. Mayorkas, 988 F.3d 8, 13 (1st Cir. 2021).

different from the search of a person.[84] The First Circuit did not agree with the ruling in *Cano* with regard to searching for evidence of contraband; it determined that the exception encompasses both advanced searches for contraband and evidence of contraband.[85] The First Circuit argued that searching for evidence of contraband is important in limiting "who and what may enter the country."[86] Under CBP policy, an officer can "detain electronic devices or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search."[87] Under ICE policy, officers can apprehend "electronic devices, or copies of information therefrom [for] a reasonable time given the facts and circumstances of the particular search."[88] The First Circuit also maintained this holding regarding detention for a reasonable period of time in *U.S. v. Montoya de Hernandez*.[89]

The major holdings to come out of this First Circuit opinion are that under the border-search exception of the Fourth Amendment, basic searches at the border do not require any level of suspicion, and advanced border searches, which are performed under a minimum of reasonable suspicion, are not limited to the search of contraband but are also extended to searches of evidence of contraband.[90]

ANALYSIS

III. The First Circuit's Ruling that Basic Searches of Electronic Devices at the Border Do Not Require Reasonable Suspicion Is Improper as the Basic Privacy Interests of the Persons Being Searched Are Unfairly Outweighed by the Government's Interest at the Border

A. *The Fourth Amendment's Reasonable Expectation of Privacy in a Person's Self, House, Papers, and Effects Extends to Electronic Devices, as in the Modern Era Electronic Devices Have Become a Part of One's Papers and Effects*

At the heart of the Fourth Amendment lies the ability to protect an individual from unreasonable searches and seizures.[91] As such, a

---

[84] *See id.* at 17.

[85] *Id.* at 21 (citing 934 F.3d at 1018).

[86] *Id.* at 20.

[87] *Id.* at 21.

[88] *Id.*

[89] Alasaad v. Mayorkas, 988 F.3d 8, 21 (1st Cir. 2021).

[90] *Id.* at 18-21.

[91] Hart, *supra* note 49, at 374–76.

government actor cannot search or seize an individual's person or property unreasonably, without cause, or without a warrant unless an exception applies.[92] Fundamentally, the introduction of the Fourth Amendment allows a person's papers, compared to their other personal effects, the greatest security from governmental abuse.[93] Since its conception, a person's "papers" evolved to mean much more; now it includes personal electronic devices.[94] Electronic devices carry a "library of . . . digital papers" which equate in importance to one's actual, physical papers.[95] Among these digital papers, individuals store personal and intimate details about their lives not limited to their conversations and photos; financial and medical information; education; debt; and more.[96] Furthermore, individuals also store their professional lives, meaning their work emails, documents, and more, in their electronic devices.[97] Allowing the government the ability to search an electronic device at the border with no level of suspicion violates the very nature of the Fourth Amendment itself.[98]

Applying the *Katz* analysis, the plaintiffs in *Alasaad* all arguably pass the test: these individuals have a reasonable expectation of privacy as they have an actual privacy interest in their electronic device, and this privacy interest is one that society deems reasonable.[99] In *Alasaad*, plaintiffs Alasaad and Merchant both experienced situations where a border patrol agent saw photos of them without their headscarves on.[100] According to the first part of the *Katz* test, Alasaad and Merchant held an actual or subjective right to privacy.[101] The First Amendment's Free Exercise clause establishes the right to practice any religion free from governmental interference.[102] When border

---

[92] Hart, *supra* note 49, at 374–76.

[93] *See* Brief of Constitutional Accountability Center as Amicus Curiae in Support of Petitioners at 3, *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021), *cert. denied sub nom. Merchant v. Mayorkas*, 210 L. Ed. 2d 964 (June 28, 2021) (No. 20-1505) [hereinafter Brief of Constitutional Accountability].

[94] *See id.* at 4.

[95] *See id.*

[96] *Id.*

[97] *See* Sales, *supra* note 47, at 1100.

[98] *See* Sales, *supra* note 47, at 1100.

[99] *Compare* Katz v. United States, 389 U.S. 347, 361 (1967), *with* Alasaad v. Nielsen, 419 F. Supp. 3d 142, 149-50 (D. Mass. 2019).

[100] *See generally* Nielsen, 419 F. Supp. 3d at 149–50.

[101] *Katz*, 389 U.S. at 361 (stating the first prong of the reasonable expectation to privacy test is that the person had an actual expectation of privacy).

[102] *See Your Right to Religious Freedom*, ACLU, https://perma.cc/3ZVY-EWRT (last visited Apr.

patrol officers went through Alasaad and Merchant's phones to see photos of the plaintiffs without their headscarves on, they encroached upon the plaintiff's subjective right to privacy to honor their religious and cultural views.[103] Specifically, Muslim women who wear headscarves have the right not to remove or be seen without their headscarves unless they so choose.[104] Alasaad and Merchant, although vocal about their concerns of the photos on their phone, nonetheless experienced their subjective right to privacy stripped from them when these officers ignored their requests and continued to search their phones.[105]

Alasaad and Merchant not only held a subjective right to privacy, this privacy right is one that society recognizes as reasonable—the second prong of the *Katz* test.[106] Many cases across many courts address the right of Muslim women to wear hijabs in places with a uniform, such as work and school.[107] In 2015, the Supreme Court ruled on the case of Samantha Elauf, a Muslim woman Abercrombie & Fitch did not employ because she wore a hijab.[108] The Court ruled that according to protections Title VII offers, "[a]n employer may not make an applicant's religious practice, confirmed or otherwise, a factor in employment decisions."[109] The right to practice religion, which includes the right to wear a headscarf, is evident not only in Title VII but also in this historic ruling.[110] As both legislation and precedent recognize this freedom, it is clear that wearing a headscarf is a privacy right that society views as reasonable.[111] Under *Katz*, Alasaad and Merchant both

---

25, 2023).

[103] *See generally Discrimination Against Muslim Women - Fact Sheet*, ACLU, https://perma.cc/BQ7Z-7DMZ (last visited Apr. 25, 2023) (stating that "Muslim women should be free to express their religious beliefs…").

[104] *See* Nida Alvi, Note, *Dressed to Oppress? An Analysis of the Legal Treatment of the First Amendment and Its Effect on Muslim Women Who Wear Hijabs*, 21 CARDOZO J.L. & GENDER 785, 788–89 (2015).

[105] *Compare Nielsen*, 419 F. Supp. 3d at 149–50 (stating that two plaintiffs were adamant about not having their phone searched for religious purposes), *with* Katz v. United States, 389 U.S. 347, 361 (1967) (providing the first prong of the expectation of privacy test).

[106] *Compare Nielsen*, 419 F. Supp. 3d at 149–50 (explaining that the plaintiffs had their phones searched even though they had photos of themselves without their headscarves on), *with Katz*, 389 U.S. at 361 (stating the second prong of the expectation of privacy test).

[107] *See* Alvi, *supra* note 104, at 791–94.

[108] E.E.O.C. v. Abercrombie & Fitch Stores, Inc., 575 U.S. 768, 770–71 (2015).

[109] *Id.* at 773.

[110] *Id.* at 775 (ruling that the plaintiff who was not hired was wrongfully discriminated against per Title VII).

[111] *See generally id.* (setting out the importance of one's right to express their religion without being discriminated against).

held a subjective privacy interest in the ability to practice their religion, and this religious practice is one that society deems as reasonable.[112]

Next, plaintiffs Dupin, Bikkannavar, and Merchant endured their reasonable expectation of privacy under *Katz* denied when border patrol officers reviewed information relating to their jobs on their electronic devices.[113] Applying the first prong of the *Katz* test, these plaintiffs held a subjective right to privacy.[114] As a journalist, Dupin holds a duty to act under the core standards of journalistic integrity.[115] As such, he must respect secrecy and privacy at all times while in this profession, especially for those individuals he receives information from.[116] As an employee of NASA, Bikkannavar's subjective right to privacy exists because he works for a company that researches and holds sensitive and highly confidential information.[117] As the owner of a media company, Merchant holds a subjective right to privacy because her electronic devices contain privileged attorney-client communications.[118] One who seeks legal advice enjoys a right to the utmost confidence that their conversation with a lawyer will remain private.[119] Therefore, in accordance with the first prong of the *Katz* analysis, these plaintiffs all held a subjective right to privacy in their electronic devices.[120]

---

[112] *Compare* Alasaad v. Nielsen, 419 F. Supp. 3d 142, 149–50 (D. Mass. 2019), *with* Katz v. United States, 389 U.S. 347, 361 (1967).

[113] *See generally Nielsen*, 419 F. Supp. 3d at 142 (showcasing that one plaintiff whose phone was examined was a journalist, and another plaintiff worked for NASA).

[114] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (stating the first part of the test is that the plaintiff had a subjective right to privacy).

[115] *See generally SPJ Code of Ethics*, SOC'Y OF PROF'L. JOURNALISTS, https://perma.cc/TYV8-6D2H (last modified Sept. 6, 2014) (outlining the four principles of ethics in journalism).

[116] *See generally Declaration of the Rights and Duties of Journalists*, ACCOUNTABLE JOURNALISM (November 23-24, 1971), https://perma.cc/Z7YQ-VF9R (listing the duties journalists must uphold while doing their job).

[117] *See generally About NASA*, NASA, https://perma.cc/3DG4-X6G7 (last visited Apr. 25, 2023) (explaining that NASA is "the global leader in space exploration" and creates important "space technologies").

[118] *Compare Nielsen*, 419 F. Supp. 3d at 149–50 (explaining the plaintiffs' circumstances with the communications they had on their device), *with Katz*, 389 U.S. at 361 (Harlan, J., concurring) (stating the two-prong expectation of privacy test).

[119] *See* Jackie Unger, *Maintaining the Privilege: A Refresher on Important Aspects of the Attorney-Client Privilege*, A.B.A (Oct. 31, 2013), https://perma.cc/DQC7-DVHZ.

[120] *Compare Nielsen*, 419 F. Supp. 3d at 149–50, *with Katz,* 389 U.S. at 361 (Harlan, J., concurring).

These plaintiffs also meet the second prong of the *Katz* analysis: that the privacy interest is one that society deems as reasonable.[121] Regarding Dupin's job as a journalist, laws such as the Newsroom Integrity Statement and the Policy on Confidential Sources require that journalists continue to uphold their ethics and obligations in their field.[122] Regarding Bikkannavar's job at NASA, many laws prevent the disclosure of information by an employee of any United States department or agency.[123] There is also Supreme Court precedent that addresses the need for lawyers to have privacy in their work and remain independent from interference or intrusion.[124] These privacy interests of employee work product of any kind, which society clearly recognizes through legislation and precedent, pass the second prong of the *Katz* test.[125]

The plaintiffs in *Alasaad* require the privacy interests allotted in *Katz*.[126] These plaintiffs did not lose their reasonable expectation of privacy just because they traveled across the border with their electronic devices.[127] These devices contained far more information than their person or luggage could ever contain.[128] In addition, the plaintiffs themselves requested border patrol agents not to search through their devices, showing their intention of privacy in their items.[129] Therefore, the plaintiffs in *Alasaad* experienced their reasonable expectation of privacy infringed when border patrol officers, with no level of suspicion, performed a search of their devices.[130]

B. *Basic Searches of Electronic Devices at the Border Must Require Reasonable Suspicion as the Scope of a Basic Search of an Electronic Device Is not Clear*

Many courts, including the First Circuit, rejected the notion that routine searches of electronic devices at the border are not intrusive in nature and

---

[121] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[122] *See generally Ethical Journalism*, N.Y. TIMES, https://perma.cc/4UFF-TC5G (last visited Apr. 25, 2023).

[123] *See, e.g.*, Disclosure of Confidential Information Generally, 18 U.S.C.A. § 1905 (West).

[124] Hickman v. Taylor, 329 U.S. 495, 510–11 (1947).

[125] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (explaining the second prong of the *Katz* test).

[126] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[127] *Compare* Alasaad v. Nielsen, 419 F. Supp. 3d 142, 149–50 (D. Mass. 2019), *with Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[128] *Nielsen*, 419 F. Supp. 3d at 163.

[129] *Id.* at 149–50.

[130] *See generally* Alasaad v. Mayorkas, 988 F.3d 8, 19 (1st Cir. 2021) (stating that reasonable suspicion is not needed for basic border searches).

therefore require no level of suspicion.[131] However, courts fail to recognize that there is no way to distinguish when a routine or basic search of an electronic device becomes non-routine or advanced.[132] CBP and ICE policy themselves are not clear on where the line is drawn between these two types of searches.[133] At the border, it is possible to have a routine search of a traveler's clothing and bags without it becoming a non-routine search.[134] A routine search is described as one which "does 'not pose a serious invasion of privacy' and 'embarrass or offend the average traveler.'"[135] The factors for whether a search is basic or advanced include: "whether the search results in the exposure of intimate body parts; . . . whether the type of search exposes the suspect to pain or danger; . . . and whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search."[136] In contrast, advanced searches have been identified "as prolonged detentions, strip searches, body cavity searches, or involuntary x-ray searches."[137] While these lines are clearer when it comes to searching a person or their physical belongings at the border (like their backpack or wallet), it is harder to apply these factors to electronic devices.[138]

Attempts to identify where the line is drawn between routine and non-routine searches of electronic devices at the border led courts to explain that, while a brief scroll through a traveler's electronic device might not require reasonable suspicion because it is a routine search, taking the electronic device away and conducting a more thorough search of the hard drive does

---

[131] Hart, *supra* note 49, at 372–73.

[132] *See* SMITH ET AL., *supra* note 2, at 21.

[133] *Compare* Border Search of Electronic Devices, Directive No. 3340-049A 4-5 (CBP Jan. 4, 2018), https://perma.cc/VKS8-ALT9 (mentioning that border searches detect evidence relating to terrorism or other crimes that threaten national security but no mention of what is looked for when searching for evidence of contraband instead of contraband itself), *with* Border Searches of Electronic Devices, Directive No. 7-6.1 3 (ICE Aug. 18, 2009), https://perma.cc/9XXK-W7PE (explaining the process ICE should go through if they find evidence of contraband, but not what they should look for when searching for evidence of contraband as opposed to contraband itself).

[134] SMITH ET AL., *supra* note 2, at 21.

[135] SMITH ET AL., *supra* note 2, at 22 (citing United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993)).

[136] SMITH ET AL., *supra* note 2, at 22 (citing United States v. Braks, 842 F.2d 509, 511–12 (1st Cir. 1988)).

[137] SMITH ET AL., *supra* note 2, at 23.

[138] *See* Hart, *supra* note 49, at 386–87.

require reasonable suspicion because then it becomes non-routine.[139] However, looking at what the First Circuit considers a routine search in *Alasaad*, it seems that there is more confusion than ever.[140] For example, after the second search by border patrol of Alasaad's phone, one of the officers inquired about a photograph that they remembered on Alasaad's phone during the first search but did not notice and assumed deleted by the second search.[141] The fact that this basic search occurred with no reasonable suspicion of contraband and led to an officer remembering the contents of Alasaad's photographs proves the intrusive nature of the search, beyond just a basic search.[142] Most likely, the same would not occur in a brief search of a person's backpack or luggage because there is less of a chance that a brief search in that case is intrusive .[143] There is an underlying difference between electronic devices and backpacks due to the nature of sensitive information electronic devices hold.[144]

Electronic devices are not closed containers, even though courts believe they are.[145] The two are not equivalent because closed containers will never reveal as much about a traveler as their electronic device, which could expose years of information in a single brief search.[146] As such, a requirement of reasonable suspicion for basic searches of electronics would protect the privacy of travelers because they would not have to worry about the exposure of their lives to border patrol simply because they are traveling.[147] Searches of electronic devices at the border must balance the interests of both the government and the traveler.[148]

---

[139] *See* Hart, *supra* note 49, at 383–84.

[140] *See* SMITH ET AL., *supra* note 2, at 49.

[141] Alasaad v. Nielsen, 419 F. Supp. 3d 142, 149 (D. Mass. 2019).

[142] *See* SMITH ET AL., *supra* note 2, at 48.

[143] *See* Hart, *supra* note 49, at 379–80.

[144] *See* Hart, *supra* note 49, at 383–84.

[145] *See* Joelle Hoffman, Article, *Reasonable Suspicion Should Be Required at a Minimum for Customs Officials to Execute a Search of a Laptop at U.S. Borders: Why U.S. v. Arnold Got It Wrong*, 36 W. ST. U.L. REV. 173, 181 (2009).

[146] *See id.* at 181–82.

[147] *See id.* at 182.

[148] *See* Hart, *supra* note 49, at 376.

C. *Although Governmental Interest Is at Its Peak at the Border, Reasonable Suspicion to Conduct Basic Searches of Electronic Devices Should Be Required So There Is Both a Balancing of Interests Between the Government's and a Person's Fourth Amendment Rights*

The border-search exception applies to what a traveler holds on their person, most notably a backpack or suitcase.[149] The border-search exception is designed to catch illegal contraband that poses an immediate danger to the country.[150] A routine or basic search of the physical contents of a backpack or suitcase, meaning opening these bags, touching and moving items around, potentially exposes illegal contraband almost immediately.[151] However, requiring no suspicion when conducting a basic search of electronic devices, which, as discussed above, contain a multitude of personal and professional information, exposes the individual to more privacy intrusion and unfairly weighs in the favor of the governmental interest among all else.[152] An equitable balancing of the scales must exist among individuals' and the government's interests when it comes to basic searches of electronic devices at the border.[153] Requiring reasonable suspicion of contraband before searching these devices, at the very least, is the correct way to balance these interests.[154]

Comparing the border-search exception to other notable Fourth Amendment exceptions highlights instances where the government's interest is more clearly balanced; basic searches of electronic devices at the border should mirror these exceptions.[155] For example, the *Terry* Court ruled that an officer must identify "specific and articulable facts, which taken together with rational inferences from those facts, reasonably warrant an intrusion," meaning a Terry stop requires reasonable suspicion before the stop occurs.[156] The overarching goal of protecting both the officers and the

---

[149] *See* Hoffman, *supra* note 145, at 177.

[150] *See* Hoffman, *supra* note 145, at 176–77.

[151] *See* Hoffman, *supra* note 145, at 182.

[152] *See* Brief of Constitutional Accountability, *supra* note 93, at 17–18.

[153] *See* Brief of Constitutional Accountability, *supra* note 93, at 13–14.

[154] *See* Hoffman, *supra* note 145, at 182.

[155] *Compare* Alasaad v. Mayorkas, 988 F.3d 8, 15 (1st Cir. 2021) (stating that the purpose of the border search exception is to catch contraband before it enters the country), *with* Terry v. Ohio, 392 U.S. 1, 23 (1968) (stating that an officer must think there is an immediate harm to himself before searching the person).

[156] *Terry*, 392 U.S. at 21.

public is served by requiring reasonable suspicion because it also balances the privacy interests of the individual.[157] Like *Terry*, requiring reasonable suspicion before conducting basic searches at the border balances both the interests of the government and the individual.[158] Furthermore, electronic devices at the border do not present nearly as much of a threat of immediate harm as contraband does.[159] It is easier to bring electronic contraband into the country and bypass the checks and balances at the border, regardless of whether this contraband is seized, by uploading it onto the cloud.[160] If this is the case, then requiring no suspicion for basic searches at the border will only serve to invade privacy interests, and not actually catch contraband.[161] Therefore, modeling basic searches of electronic devices at the border after *Terry* is one way to ensure the balance of interests.[162]

Another Fourth Amendment exception that the border-search exception could mirror is the search of a cell phone following a search incident to arrest.[163] The Ninth Circuit ruled that due to the amount of information a cell phone holds, a warrant is required to uphold protections granted to individuals from the Fourth Amendment.[164] A balance between the governmental interests supporting no suspicion and the Ninth Circuit's reasoning for requiring a warrant is to require reasonable suspicion for a basic search.[165] That way, there is a true balancing of two sides that vary in interests.[166] Overall, requiring reasonable suspicion to conduct basic searches at the border is the appropriate way to safeguard both individuals' privacy interests and the government's heightened interest in keeping contraband out of the country.[167]

---

[157] *Id.* (explaining how the interests of both the government and the individual are protected).

[158] *Compare Mayorkas*, 988 F.3d at 18, *with Terry*, 392 U.S. at 21.

[159] *See generally* Riley v. California, 573 U.S. 373, 399 (2014) (explaining that cell phone searches in a non-border setting require a warrant because cell phones were not an immediate danger to police officers).

[160] *See* Hoffman, *supra* note 145, at 182–83.

[161] *See* Hoffman, *supra* note 145, at 182–83.

[162] *Compare* Alasaad v. Mayorkas, 988 F.3d 8, 18 (1st Cir. 2021), *with Terry*, 392 U.S. at 21 (1968).

[163] *See Riley*, 573 U.S. at 373.

[164] *See generally id.* (ruling that since a cell phone is not an immediate danger unless it is used as a weapon, a warrant is required to search it).

[165] *Compare id.* (explaining that searching electronic devices requires a warrant), *with Mayorkas*, 988 F.3d at 18 (implying that because governmental interest is at its peak at the border, there is no balance with individual rights).

[166] *See* Hoffman, *supra* note 145, at 185.

[167] *Compare Mayorkas*, 988 F.3d at 13 (affirming the government's interest to keep contraband out of the country), *with* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring)

IV. The First Circuit's Ruling That Advanced Searches of Electronic Devices at the Border Included Searching for Evidence of Contraband Is Inappropriate as It Sets No Clear Guidelines of What Border Patrol Agents Should Regard as Evidence and Grants These Agents High Discretionary Power Over a Person's Electronic Device

A. *Advanced Searches of Electronic Devices at the Border Should Only Include Searching for Contraband, not "Evidence of Contraband"*

Massachusetts law distinguishes "evidence of contraband" by stating that "[e]vidence is an item that is otherwise lawfully possessed but could be used to explain the government's theory of the case."[168] Contraband, on the other hand, is something that is always unlawful, such as carrying a switchblade.[169] Regarding electronic devices, it is unclear what "evidence of contraband" means, as the Ninth Circuit noted a difference between a search for contraband and a search for evidence of contraband.[170] Border patrol agents do not have a "general authority to search for crime."[171] For example, texts or emails used as evidence for the crime of price fixing are themselves not contraband, but rather evidence of a crime.[172] In *Cano*, the defendant's cell phone contained phone numbers which officers wrote down, and proceeded to call these numbers.[173] The court noted they can point to no law that states it is a specific crime to bring in evidence of contraband, as that itself is so broad.[174] The Supreme Court has stated that seizure of goods prohibited at the border is inherently different from seizure of goods which could be used as evidence in prosecuting crimes.[175] Additionally, the Supreme Court has recognized that "[t]he scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible."[176]

(expressing the importance of maintaining an individual's reasonable privacy interest).

[168] Victoria L. Nadela & Roger Witkin, 42 Mass. Prac., Criminal Defense Motions § 6:4 (5th ed. 2021).

[169] *Id.*

[170] United States v. Cano, 934 F.3d 1002, 1017 (9th Cir. 2019).

[171] *Id.*

[172] *Id.*

[173] *Id.* at 1008–09.

[174] *See id.* at 1017.

[175] *See* Boyd v. United States, 116 U.S. 616, 623 (1886).

[176] Terry v. Ohio, 392 U.S. 1, 19 (1968).

In the Ninth Circuit, a border patrol agent must stop their search at actual digital contraband, such as child pornography, which is a widely accepted use of the border-search exception.[177] However, beyond actual contraband itself, a border patrol agent must obtain a warrant if they want to search for evidence of contraband.[178] This narrows the scope beyond a search-for-anything approach and sets actual parameters on these advanced searches—no contraband, no more search.[179] The First Circuit must model its policy on advanced searches at the border to only contain searching for contraband, not evidence of contraband, rather than upholding this broad policy.[180] In addition to the confusion brought about by judicial precedent, CBP and ICE policy themselves do not provide guidelines as to what "evidence of contraband" entails.[181]

The First Circuit's failure to prohibit searches for "evidence of contraband" in electronic devices at the border is a slippery slope: by expanding the already set precedent on only looking for contraband during advanced searches, individuals' Fourth Amendment rights will be significantly harmed.[182] The First Circuit, or even the Supreme Court, must no longer allow searching for evidence of contraband for this very reason.[183] If contraband, like child pornography, is not apparent during an advanced search, then the search must stop altogether, with only a warrant allowing it to continue.[184] This way, border patrol authority to search electronic devices remains limited at the border.[185]

---

[177] Kristina Davis, *Returning from Travel Abroad? A Court Put Limits on Border Officers Rummaging Through Your Phone*, SAN DIEGO UNION-TRIB. (July 24, 2021, 6:00 AM PT), https://perma.cc/N33A-N5TC.

[178] *Id.*

[179] *See id.*

[180] *See generally id.* (stating that the First Circuit did not agree with the "narrow view in *Cano*").

[181] *Compare* Border Search of Electronic Devices, Directive No. 3340-049A 9 (CBP Jan. 4, 2018), https://perma.cc/VKS8-ALT9 (explaining only what type of contraband officers look for, not what evidence of contraband entails), *with* Border Searches of Electronic Devices, Directive No. 7-6.1 3 (ICE Aug. 18, 2009), https://perma.cc/9XXK-W7PE (analyzing only the process officers go through when finding evidence of contraband).

[182] *Recent Cases supra* note 1, at 1468.

[183] *See Recent Cases supra* note 1, at 1468.

[184] Davis, *supra* note 177.

[185] *See* Davis, *supra* note 177.

B. *With No Set Guidelines of What "Evidence of Contraband" Entails, There Is a High Probability That Border Patrol Agents Will Abuse Their Power During These Searches and Seizures*

The creation of the U.S. Border Patrol is rooted in racism.[186] While this began with the Chinese Exclusion Act, many other migrants felt inequity while attempting to enter the country.[187] There have been many incidents "of agents using racial slurs, sexual comments, and other offensive language."[188] In fact, border patrol agents are required to use racist terms in order to make those trying to cross the border feel less than human.[189] Many complaints and lawsuits have been filed against the border patrol for incidents such as targeting migrants because of their skin and hair color, and stopping cars of Black U.S. citizens because of their skin color without giving a legitimate reason for the stop.[190] This is another reason to limit the authority of border patrol agents to conduct searches of electronic devices at the border; the system is already so corrupt that only clear parameters will ensure minimal abuse of power.[191]

In general, CBP officers are required to uphold the values of the Fourth Amendment, which precludes unreasonable searches and seizures.[192] Since 2010, more than 230 people died at the hands of CBP — their cause of death is unclear as a result of either no media attention or no transparency by border patrol.[193] Young individuals make up a substantial percentage of those killed — with 15% being between the ages of 18 to 29.[194] Additionally, CBP specializes in the use of excessive force.[195] A 2013 investigation into this

---

[186] KATY MURDZA & WALTER EWING, THE LEGACY OF RACISM WITHIN THE U.S. BORDER PATROL 4 (2021), https://perma.cc/4PHG-EGJ6.

[187] *Id.* at 6.

[188] *Id.* at 4.

[189] *Id.* at 13.

[190] *Id.* at 14.

[191] *See generally id.* at 5 (explaining that a lot must be done by the Biden Administration in order to change the ways of border patrol).

[192] *Arrests/Searches & Seizures*, HOLD CBP ACCOUNTABLE, https://perma.cc/9JK5-SZVN (last visited Apr. 25, 2023).

[193] *Abuse of Power and its Consequences*, SOUTHERN BORDER COMMUNITIES COALITION (SBCC), https://perma.cc/5K9S-XRGE (last updated Aug. 11, 2022) [hereinafter *Abuse of Power*].

[194] *Id.*

[195] *See id.*

issue forced CBP to update its use-of-force handbook.[196] However, data shows that the border patrol agency and its officers still face little to no consequences for their violent actions.[197] Furthermore, in what's known as the 100-mile enforcement zone, Border Patrol manages at least one hundred temporary and permanent checkpoints.[198] At these checkpoints, "drivers can be stopped and questioned to verify their lawful status."[199] However, due to the amount of authority Border Patrol holds, a myriad of evidence revealed that these checkpoints not only "violate constitutional rights [but also] lead to abuse."[200]

Department of Homeland Security Secretary Alejandro Mayorkas made a commitment to break from Trump's racist and anti-immigrant policies.[201] While Secretary Mayorkas attempted to stop the abuse of power by ICE by directing the agency to focus its resources on threats to national security, public safety, and distributing guidance on which groups remain a priority for immigration enforcement, he failed to restrict ICE's authority in many other instances.[202] ICE agents abuse their power by arresting groups of people who they deem to be priorities, but they are not considered priorities according to the criteria set forth by Secretary Mayorkas.[203]

Border patrol agents wide authority to search for evidence of contraband in electronic devices at the border because gives them too much discretion to search electronic devices for whatever they want, and for however long they want.[204] In *Alasaad*, Wright, a computer programmer, had his computer extracted and CBP retained the data for a period of 56 days.[205] It is unclear what border patrol officials thought they would find, but this was potentially an instance of abuse of power by border patrol agents.[206]

---

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] *Id.*

[200] *Id.*

[201] Naureen Shah & Jonathan Blazer, *Secretary Mayorkas Pledged to End His Agency's Anti-Immigrant Abuses. Here's What He's Delivered*, ACLU (July 21, 2021), https://perma.cc/JS4W-LMB2.

[202] *Id.*

[203] *See id.*

[204] *See generally Abuse of Power*, *supra* note 193 (explaining border authorities' broad range of power).

[205] Alasaad v. Nielsen, 419 F. Supp. 3d 142, 150 (D. Mass. 2019).

[206] *Compare* Alasaad v. Mayorkas, 988 F.3d 8, 20–21 (1st Cir. 2021) (failing to mention what evidence of contraband is), *with Abuse of Power*, *supra* note 193 (stating how border patrol officers regularly abuse their power).

Therefore, this longstanding abuse of power that border patrol agents regularly exhibit, along with the failure of law enforcement to rein this abuse in, showcases that searching for evidence of contraband in electronic devices must remain outside the scope of border searches.[207]

CONCLUSION

In today's modern age, electronic devices will only continue to develop, far into the future. There is growing turmoil in the United States on how to handle them at the border. The First Circuit decided in *Alasaad v. Mayorkas* that basic, routine searches at the border required no reasonable suspicion and that advanced, non-routine searches at the border required reasonable suspicion with an expanded scope of not just searching for contraband, but also evidence of contraband. The First Circuit failed to set precedent to protect both the government's privacy interests as well as the privacy interests of the people. The First Circuit should have ruled that basic searches of electronic devices at the border require reasonable suspicion. It is clear under the *Katz* analysis that the plaintiffs in this case held a reasonable expectation of privacy that was taken away from them. Furthermore, the line between basic and advanced searches of electronic devices is so nuanced that some argue that the search of electronic devices in general is an advanced search. If the First Circuit required reasonable suspicion for both basic and advanced searches, it would clear up this confusion. Additionally, there is an unfair balancing of interests; other Fourth Amendment exceptions balance interests between the government and the individual more equally, and the border-search exception for electronic devices should do the same.

Moreover, the First Circuit should have decided that the search of electronic devices at the border stops at searching for contraband and does not extend to evidence of contraband. The term "evidence of contraband" is very unclear (even though some courts have defined it) because the scope of what is searched for or what is regarded as "evidence of contraband" is incredibly ambiguous. It allows for an abuse of power by both CBP and ICE because even when the authority is clear, border patrol agents still abuse their power. As such, "evidence of contraband" should not be included in

---

[207] *Compare Mayorkas*, 988 F.3d at 19 (allowing for evidence of contraband to be searched for at the border), *with Abuse of Power, supra* note 193 (giving examples of many times when border patrol agents went beyond the scope of their authority).

border searches of electronic devices. Overall, the First Circuit missed a historic opportunity to correctly define the bounds of border searches of electronic devices, and this is the exact reason why the Supreme Court needs to act to correct these wrongs.