St. John's Law Review

Volume 93
Number 2 *Volume 93, 2019, Number 2*

Article 2

January 2020

Unlimited Data Search Plan: Warrantless Border Search of Mobile Device Data Likely Unconstitutional for Violating the Fundamental Right to Informational Privacy

Atanu Das

ARTICLES

UNLIMITED DATA SEARCH PLAN: WARRANTLESS BORDER SEARCH OF MOBILE DEVICE DATA LIKELY UNCONSTITUTIONAL FOR VIOLATING THE FUNDAMENTAL RIGHT TO INFORMATIONAL PRIVACY

ATANU DAS[†]

INTRODUCTION

The Fifth and Fourteenth Amendments provide United States citizens the protection of fundamental rights under their respective Due Process Clauses.[1] These fundamental rights

[†] Distinguished Scholar, Loyola University Chicago, School of Law. The views in this Article are the author's own. Special thanks to Dean Michael Kaufman, Professor Barry Sullivan, Professor Spencer Waller, Professor Sacha Coupet, and Professor John Breen for their expertise, insight, and encouragement with regard to this Article. Also, I am grateful to my Research Assistants, Jessica Sos and Nina Hintlian, who assisted me with editing, cite-checking, and researching of this Article. In addition, I would like to thank the wonderful editorial board and staff at the *St. John's Law Review*. Finally, my heartfelt thanks for the support and encouragement of my three sons, Roshan, Finn, and Leo, as well as the constant support and encouragement of my wife Noreen, without which I would not be able to complete this work.

[1] *See* Obergefell v. Hodges, 135 S. Ct. 2584, 2602 (2015) (finding "[t]he right to marry is fundamental as a matter of history and tradition, but rights come not from ancient sources alone. They rise, too, from a better informed understanding of how constitutional imperatives define a liberty that remains urgent in our own era. Many who deem same-sex marriage to be wrong reach that conclusion based on decent and honorable religious or philosophical premises, and neither they nor their beliefs are disparaged here. But when that sincere, personal opposition becomes enacted law and public policy, the necessary consequence is to put the imprimatur of the State itself on an exclusion that soon demeans or stigmatizes those whose own liberty is then denied. Under the Constitution, same-sex couples seek in marriage the same legal treatment as opposite-sex couples, and it would disparage their choices and diminish their personhood to deny them this right."); *see also* Lawrence v. Texas, 539 U.S. 558, 593 (2003) (Scalia, J. dissenting) (explaining "[o]ur opinions applying the doctrine known as 'substantive due process' hold that the Due Process Clause prohibits States from infringing *fundamental* liberty interests, unless the

likely include the right to informational privacy—the right to keep one's personal information private.[2] The claim that the right to informational privacy is fundamental is further bolstered by recent United States Supreme Court cases finding that personal data, such as email and social media, accessible through a mobile device, require a heightened level of constitutional protection.[3]

The government intrudes on the right to informational privacy when the Department of Homeland Security ("DHS") invokes the border search exception to conduct warrantless searches of United States citizens' mobile device data at the

---

infringement is narrowly tailored to serve a compelling state interest" (emphasis in original)); Washington v. Glucksberg, 521 U.S. 702, 720 (1997) (stating "[t]he [Due Process] Clause also provides heightened protection against government interference with certain fundamental rights and liberty interests," including, but not limited to, the right to marry, the right to direct the education and upbringing of one's children, the right to marital privacy, the right to use contraception, and the right to refuse lifesaving medical treatment); RONALD D. ROTUNDA & JOHN E. NOWAK, 2 TREATISE ON CONSTITUTIONAL LAW – SUBSTANCE AND PROCEDURE, § 15.7 (last updated May 2019) ("Today the Justices of the Supreme Court will apply strict forms of review under the due process clauses and the equal protection clause to any governmental actions which limit the exercise of 'fundamental' constitutional rights.").

[2] Whalen v. Roe, 429 U.S. 589, 598–600 (1977) ("The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.").

[3] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) ("We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of [cell site location information], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment."); Riley v. California, 573 U.S. 373, 403 (2014) ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life,' . . . The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant." (internal citation ommitted)*; see* Atanu Das, *Crossing the Line: Department of Homeland Security Border Search of Mobile Device Data Likely Unconstitutional*, 22 U. PA. J. L. & SOC. CHANGE 205, 239 (2019) ("Although the U.S. Supreme Court has opined that the Border Search Exception has limits without providing further guidance, established Fourth Amendment jurisprudence and recent U.S. Supreme Court case law provides the guidance that may require CBP officials to obtain a warrant based on probable cause prior to conducting a border search of mobile device data. Failure to do so would likely be unconstitutional.").

border.[4] The border search exception doctrine states that a government official or law enforcement officer can conduct a warrantless search of a person and his belongings when entering the United States at the border to determine whether the person can legally enter the country or is carrying contraband.[5]

---

[4] Emanuella Grinberg & Jay Croft, *American NASA Scientist Says His Work Phone Was Seized at Airport*, CNN (Feb. 15, 2017), https://www.cnn.com/2017/02/13/us/citizen-nasa-engineer-detained-at-border-trnd/index.html ("Facing the risk of detention and seizure of his phone [Bikkannavar] turned it over along with the PIN. He waited in a holding area with other detainees until CBP officers returned his phone and released him."); *see also* Amended Complaint at 2, Alasaad v. Duke, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017) (explaining "CBP and ICE have searched the mobile electronic devices of tens of thousands of individuals, and the frequency of such searches has been increasing. While border officers conduct some searches manually, they conduct other searches with increasingly powerful and readily available forensic tools, which amplify the intrusiveness and comprehensiveness of the searches . . . . The effect of searches of mobile electronic devices on individual privacy and expression can hardly be overstated. Travelers' electronic devices contain massive amounts of personal information, including messages to loved ones, private photographs of family members, opinions and expressive material, and sensitive medical, legal, and financial information. The volume and detail of personal data contained on these devices provides a comprehensive picture of travelers' private lives, making mobile electronic devices unlike luggage or other items that travelers bring across the border."); *Inspection of Electronic Devices*, U.S. CUSTOMS AND BORDER PROTECTION https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf (last visited Mar. 1, 2018) ("All persons, baggage, and merchandise arriving in, or departing from, the United States are subject to inspection, search and detention. This is because CBP officers must determine the identity and citizenship of all persons seeking entry into the United States, determine the admissibility of foreign nationals, and deter the entry of possible terrorists, terrorist weapons, controlled substances, and a wide variety of other prohibited and restricted items . . . . You're receiving this sheet because your electronic device(s) has been detained for further examination, which may include copying.").

[5] United States v. Ramsey, 431 U.S. 606, 617 (1977) ("This interpretation, that border searches were not subject to the warrant provisions of the Fourth Amendment and were 'reasonable' within the meaning of that Amendment, has been faithfully adhered to by this Court."); *see* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 319 (2015) ("Under [a] narrow approach, the border search exception exists to allow the government to keep out items that should be outside the United States . . . . The underlying right is to control what enters . . . the country."); *see also* Thomas Mann Miller, Note, *Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943, 1996 (2015) (stating that an individual's privacy interest in his digital data content needs to be balanced with the traditional government interest of preventing people without a legal right to enter the U.S. from crossing the border and preventing contraband from entering the country); Das, *supra* note 3, at 209 ("The initial rationale of the Border Search Exception doctrine justifies CBP officials conducting a warrantless search of a person and the person's belongings only to ascertain whether the person can legally enter the U.S. and that they are carrying no contraband. These should be construed to be are [sic] the metes and bounds of the purpose for a warrantless border search.")

The current administration has made it clear that securing the border is one of its highest priorities.[6] Border security in the current administration includes securing the border both from undocumented immigrants entering this country for a better way of life and from terrorists who may want to cause harm.[7] The Federal Bureau of Investigation ("FBI") defines a terrorist as a person with an ideology that includes committing an act of violence against a country or its people for a political cause.[8] The current administration believes the search of a person's mobile device data, including data stored remotely but accessible via the mobile device, can allow Customs and Border Patrol ("CBP") officials to determine whether the person is a terrorist and to permit CBP to detain the person, thereby preventing the person from entering the country.[9] The United States government also attempts to restrict entrance by promulgating stricter border security rules and regulations and by implementing detail oriented vetting in the immigration process.[10] DHS rules

---

[6] S.M., *Donald Trump's Travel Ban Heads Back to the Supreme Court*, THE ECONOMIST (Jan. 23, 2018) https://www.economist.com/democracy-in-america/2018/01/23/donald-trumps-travel-ban-heads-back-to-the-supreme-court; Christina Wilkie & Tucker Higgins, *Trump on Closing the US-Mexico Border: 'Security Is More Important to Me Than Trade*,' CNBC (last updated Apr. 3, 2019, 7:16 AM), https://www.cnbc.com/2019/04/02/trump-on-closing-border-security-is-more-important-to-me-than-trade.html.

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

[8] *See* Roberto Iraola, *Terrorism, the Border, and the Fourth Amendment*, 2003 FED. CTS. L. REV. 1, *V.1 (2003) ("The border exception to the Fourth Amendment provides the government with the necessary flexibility to detain and search persons and goods in its endeavor to protect the mainland and its citizens against acts of terrorism."); *see also What We Investigate: Terrorism*, FBI, https://www.fbi.gov/investigate/terrorism (last visited Aug. 6, 2019) ("International terrorism: Perpetrated by individuals and/or groups inspired by or associated with designated foreign terrorist organizations or nations (state-sponsored) . . . . [I]nspired by multiple extremist ideologies[.] . . . Domestic terrorism: Perpetrated by individuals and/or groups inspired by or associated with primarily U.S.-based movements that espouse extremist ideologies of a political, religious, social, racial, or environmental nature.").

[9] *See Inspection of Electronic Devices*, *supra* note 4; *see also* Das, *supra* note 3, at 210.

[10] *Trump's Executive Order: Who Does Travel Ban Affect?* (Feb. 10, 2017), BBC, http://www.bbc.com/news/world-us-canada-38781302 ("All travellers who have nationality of Iran, Iraq, Libya, Somalia, Sudan, Syria and Yemen are not permitted to enter the US for 90 days, or be issued an immigrant or non-immigrant visa.").

promote this border security policy by likely unconstitutionally expanding the border search exception doctrine to more than determining whether a person can legally enter the United States and whether the person's belongings include contraband.[11] The DHS rules use the border search exception doctrine to justify expanding a warrantless border search to determine whether the person is a terrorist.[12] DHS personnel, including CBP officials, as well as the courts, seize on the broad language of case law pertaining to border searches to expand the limits of the border search exception doctrine.[13] This expansive application of the doctrine gives CBP officials almost unlimited scope to conduct warrantless border searches of a person and the person's belongings.[14] However, the DHS and the courts have wrongly interpreted the border search exception doctrine.[15]

The underlying rationale for the border search exception is that it is reasonable to search a person and the person's belongings at the border without a warrant to determine whether the person has a right to enter the country or is carrying contraband.[16] The border search exception doctrine views the border or point of entry—that is, an airport or ship dock—as a place for protecting both the nation's sovereignty and the person's privacy.[17] The border search exception doctrine should

---

[11] *See Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices*, DEPARTMENT OF HOMELAND SECURITY, https://www.dhs.gov/publication/border-searches-electronic-devices; *see also* Iraola, *supra* note 8, at I.6; *Inspection of Electronic Devices*, *supra* note 4.

[12] *See Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices*, *supra* note 11*; see also* Iraola, *supra* note 8; *Inspection of Electronic Devices*, *supra* note 4; Motion to Dismiss at 3–4, Alasaad v. Duke, No. 1:17-cv-11730 (D. Mass. Dec. 15, 2017) [hereinafter Motion to Dismiss].

[13] WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, § 10.5(a) (5th ed. 2017) ("Any person or thing coming into the United States is subject to search by that fact alone, whether or not there be any suspicion of illegality directed to the particular person or thing to be searched" (citing United States v. Odland, 502 F.2d 148, 151 (7th Cir. 1974))).

[14] United States v. Cotterman, 709 F.3d 952, 970 (9th Cir. 2013); United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005); United States v. Saboonchi, 990 F. Supp. 2d 536, 570–71 (D. Md. 2014). These cases all hold that digital data content from respective defendants' electronic devices can be lawfully searched without a warrant based only on reasonable suspicion.

[15] *See* United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977) (stating that "a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out," thereby finding that CBP officials do not have unbridled authority to conduct a border search for any purpose).

[16] Carroll v. United States*,* 267 U.S. 132, 153–54 (1925).

[17] *Id.*; *see also* Miller, *supra* note 5, at 1992; Kerr, *supra* note 5, at 294–95 ("The Supreme Court has held that a border search exception to the Fourth Amendment

take into account both the threat from individuals attempting to enter illegally or to smuggle contraband and that an individual's privacy interests are vulnerable to border security officials.[18]

Courts and some legal commentators have been reluctant to impose any limit on warrantless border searches of mobile device data or other electronic data based on the border search exception doctrine under the Fourth Amendment.[19] However, framing warrantless border searches of mobile device data as a governmental intrusion on a fundamental right, namely the right to informational privacy, may shield mobile device data from the CBP officials' prying eyes. The Supreme Court has found that the right to decisional privacy—to make certain decisions about one's life without governmental interference—is a fundamental right and subject to strict scrutiny.[20] However, the Court has waffled as to whether the right to informational privacy is a fundamental right subject to the same level of strict scrutiny.[21] This Article argues that the right to informational privacy is a fundamental right for three reasons. First, the right to

---

applies to property entering and exiting the United States at the border, as well as its functional equivalent, in order to protect the sovereign interests of the United States in monitoring what enters and exits the country.").

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

[19] *Ramsey*, 431 U.S. at 618 n.13*; see, e.g.*, Eunice Park, *The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post-Riley*, 44 HASTINGS CONST. L.Q. 277, 314 (2017) (stating "this Article urges that such a [reasonable suspicion] standard provides the balance that is needed between the critical interests of both law enforcement and the private individual").

[20] *See* Washington v. Glucksberg, 521 U.S. 702, 720 (1997)*; see also* ROTUNDA & NOWAK, *supra* note 1 ("There is a fundamental right to privacy which includes various forms of freedom of choice in matters relating to the individual's personal life. This right to privacy has been held to include rights to freedom of choice in marital decisions, child bearing, and child rearing.").

[21] NASA v. Nelson*,* 562 U.S. 134, 158–59 (2011) (subjecting the government intrusion to the right to informational privacy to something less than strict scrutiny); Nixon v. Adm'r of Gen. Servs.*,* 433 U.S. 425, 465 (1977) (implicitly explaining that any government intrusion of the right to informational privacy is subject to strict scrutiny, but the Act in this case had a screening process to limit materials that would be public based on whether it dealt with personal information of President Nixon, such that it was sufficiently narrowly tailored to the compelling government interest); Whalen v. Roe, 429 U.S. 589, 603–04 (1977) (stating "[w]e hold that neither the patient-identification requirements in the New York State Controlled Substances Act of 1972 . . . is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment").

informational privacy for mobile device data is equally as important as the right to decisional privacy.[22] Thus, if the right to decisional privacy is a fundamental right, then logic follows that the right to informational privacy also constitutes a fundamental right.[23] Second, recent Supreme Court cases have held that mobile device data receives heightened constitutional protection.[24] Third, the Supreme Court's rationale for giving mobile device data heightened constitutional privacy protection stems from the same Supreme Court jurisprudence that produced the right of informational privacy.[25] If mobile device data receives heightened protection and properly falls within the scope of the fundamental right of informational privacy, any government intrusion into an individual's mobile device data which is not narrowly tailored to a compelling governmental interest would violate the Fifth Amendment.

Part I of this Article discusses a case in which a United States citizen was subject to an unconstitutional warrantless border search of his mobile device data. Part II explains the history and current state of Supreme Court jurisprudence of the border search exception doctrine. Part III explains the way in which Supreme Court jurisprudence finds the right to informational privacy for mobile device data to be a fundamental right. Part IV discusses the reluctance of some legal commentators to find that a governmental intrusion on the right to informational privacy is subject to strict scrutiny. Part V finds that a warrantless border search of mobile device data is likely unconstitutional for violating the right to informational privacy under the Due Process Clause of the Fifth Amendment.

---

[22] Mary D. Fan, *Constitutionalizing Informational Privacy by Assumption*, 14. U. PA. J. CONST. L. 953, 966–7 (March 2012) (citing *Whalen*, 429 U.S. at 599–600).

[23] *Id.*

[24] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Riley v. California, 573 U.S. 373, 403 (2014).

[25] *See* Olmstead v. United States, 277 U.S. 438, 474–75 (1928) (Brandeis, J., dissenting) (stating "with reference to Lord Camden's judgment in Entick v. Carrington, 19 Howell's State Trials, 1030: 'The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case there before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctities of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . . In this regard the Fourth and Fifth Amendments run almost into each other.'"); *see also Carpenter*, 138 S. Ct. at 2223.

I. WARRANTLESS SEARCH OF A UNITED STATES-BORN CITIZEN'S MOBILE DEVICE DATA BY AIRPORT BORDER SECURITY

In January 2017, thirty-five-year-old American-born Sidd Bikkannavar was detained at Houston's George Bush Intercontinental Airport while returning from a trip abroad.[26] During the conducting of customs and immigration procedures, CBP officials insisted on searching his mobile phone data.[27] Initially, he did not comply with CBP officials, as he worked for the National Aeronautics and Space Administration's ("NASA") Jet Propulsion Laboratory ("JPL") as a scientist in Pasadena, California, and his mobile phone data included confidential information regarding his work for NASA.[28] However, as CBP officials clearly indicated that his mobile phone could be seized indefinitely until he complied with their demands, Bikkannavar consented for CBP officials to search his mobile phone data.[29]

Bikkannavar stated that CBP officials gave him a document titled "Inspection of Electronic Devices," which indicated that the CBP had the right to search all people, baggage, and merchandise arriving to, or departing from, the United States.[30] Further, it indicated that such a search was mandatory and that failure to cooperate could lead to the seizure of the mobile phone.[31] In addition, the rules indicated that border searches of mobile device data sought to determine whether a person entering the United States had a terrorist ideology and to deter terrorists from entering the country.[32]

Ironically, Bikkannavar underwent two previous background checks to determine his risk to national security.[33] He went through a thorough background check to work with confidential information at NASA.[34] Further, he had also submitted himself

---

[26] Grinberg and Croft, *supra* note 4; *see also* Das, *supra* note 3, at 211.

[27] Kaveh Waddell, *A NASA Engineer Was Required to Unlock His Phone at the Border*, THE ATLANTIC (Feb. 13, 2017), https://www.theatlantic.com/technology/archive/2017/02/anasaengineerisrequiredtounlockhisphoneattheborder/516489.

[28] Waddell, *supra* note 27.

[29] Grinberg & Croft, *supra* note 4.

[30] Waddell, *supra* note 27; *see also* Amended Complaint, *supra* note 4, at 21–22.

[31] Waddell, *supra* note 27.

[32] *Inspection of Electronic Devices*, *supra* note 4; *see* Motion to Dismiss, *supra* note 12, at 2–3.

[33] *See* Waddell, *supra* note 27; *see also* Das, *supra* note 3, at 212.

[34] *See* Waddell, *supra* note 27.

to another background check as part of the Global Entry program that allows officials to expedite customs procedures after a fingerprint scan.[35]

In September 2017, several coplaintiffs, including Bikkannavar, represented by the American Civil Liberties Union ("ACLU"), filed suit against the DHS in Federal District Court in Massachusetts on the theory that warrantless border search of mobile device data by CBP officials is unconstitutional under both the First and Fourth Amendments.[36] The plaintiffs did not argue the warrantless border search of mobile device data was an unconstitutional government intrusion of the fundamental right of informational privacy under the Due Process Clause of the Fifth Amendment. As discussed herein, had the plaintiffs made such a claim, the court should find in their favor.

II. BORDER SEARCH EXCEPTION DOCTRINE JURISPRUDENCE

The purpose of the border search exception doctrine is to balance the sovereign's interest in protecting the nation from the unlawful entry of people and contraband against a person's reasonable expectation of privacy in his person and his belongings.[37] It allows CBP officials to conduct a reasonable search, without a warrant, of a person and his belongings at the border.[38]

The border search exception doctrine was first introduced by the Supreme Court in *Carroll v. United States*.[39] In this 1925 case, law enforcement officers detained driver George Carroll and searched his vehicle for liquor, which was considered to be contraband during the Prohibition, within the interior of Michigan, not near the United States-Canadian border.[40] After observing Carroll for months during a sting operation, the law enforcement officers suspected him of transporting liquor illegally such that, one day, the law enforcement officers stopped

---

[35] *See Id.*

[36] *See* Amended Complaint, *supra* note 4, at 11; *see also* Das, *supra* note 3, at 212.

[37] Carroll v. United States, 267 U.S. 132, 154 (1925); *see* Miller, *supra* note 5, at 1996; Das, *supra* note 3, at 209.

[38] *See* Iraola, *supra* note 8, at *V.1.

[39] 267 U.S. at 154 (1925); *see also* LaFave, *supra* note 13 (stating that "the United States Supreme Court did not have occasion . . . to pass directly upon the question of whether routine searches of persons or things entering the country are permissible under the Fourth Amendment" until *Carroll v. United States*).

[40] *Carroll*, 267 U.S. at 160.

and searched the suspect's vehicle and found several dozen bottles of liquor.[41] The Court found the law enforcement officers' suspicion from the sting operation to be sufficient probable cause to conduct a warrantless search of Carroll's vehicle.[42] Although the case dealt with a vehicle stop, the Court stated that there were several exceptions to the Fourth Amendment requirement for a warrant, including a vehicle stop and a border search.[43]

Chief Justice Taft, authoring the opinion of the Court,[44] stated "the Fourth Amendment protects a person from *unreasonable* searches and seizures" when law enforcement officers fail to obtain a warrant.[45] The Court found "it would be reasonable to stop and search a vehicle without a warrant because a vehicle can move out of the jurisdiction before the law enforcement officer can obtain a warrant."[46] Thus, the Court held that to search a suspect's vehicle without a warrant is reasonable if the law enforcement officer has probable cause to do so.[47]

Further, Chief Justice Taft went on to explain the border search exception doctrine: "Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."[48] Thus, the border search exception was born in the context of a vehicle stop and the accompanying concern that a suspect may flee the jurisdiction before law enforcement can obtain a search warrant.[49] Moreover, the Court explains that "[t]he Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens."[50] Therefore, the rationale behind the border search exception is that it is in the public interest to ascertain a person's right to enter the United States and to

---

[41] *Id.* at 160.
[42] *Id.* at 162.
[43] *Id.* at 153–54.
[44] *Id.* at 143.
[45] *Id.* at 147–49; *see also* Das, *supra* note 3, at 217.
[46] *Id.* at 153–54.
[47] *Id.*
[48] *Carroll*, 267 U.S. at 154; LaFave, *supra* note 13 (stating that border searches, since the adoption of the Fourth Amendment, have been considered "reasonable" by the fact that the person or item in question has entered the country from outside).
[49] *Carroll*, 267 U.S. at 153–54; *see also* Das, *supra* note 3, at 217.
[50] *Carroll*, 267 U.S. at 149.

search, without a warrant, to determine whether the person's possessions include contraband, because any suspect may flee the jurisdiction prior to a search warrant being obtained.[51]

The DHS also uses *United States v. Montoya de Hernandez* to justify warrantless border searches of mobile device data. In that case, CBP officials at Los Angeles International Airport suspected Montoya de Hernandez of smuggling drugs in her alimentary canal.[52] When they searched her, they determined that she was wearing a girdle and elastic underpants lined with paper towels—indications of drug smuggling; from this evidence, CBP officials obtained a warrant to conduct a rectal search, after which it was found that Montoya de Hernandez was indeed smuggling drugs in her alimentary canal.[53]

Justice Rehnquist, writing for the Court, upheld the warrantless border search in that case because the "balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border."[54] Finally, the Court found "that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal."[55]

In contrast, Justice Brennan, in dissent, harshly criticized the majority opinion, stating that the search and seizure of Montoya de Hernandez were those of a police state and not indicative of the freedoms and values of this country.[56] With this decision, Justice Brennan was afraid that overzealous officers might circumvent people's Fourth Amendment protections and illegally search and seize them at the border.[57]

Although there have been invasive warrantless border searches ostensibly justified by the border search exception doctrine, as indicated by Supreme Court jurisprudence, the border search exception doctrine only allows for law enforcement officials at the border to conduct a warrantless border search to

---

[51] *Carroll*, 267 U.S. at 153–54; *see also* Kerr, *supra* note 5, at 319.

[52] 473 U.S. 531, 536–37 (1985).

[53] *Id.* at 534.

[54] *Montoya de Hernandez*, 473 U.S. at 540 (internal citations omitted); *see also* Das, *supra* note 3, at 219.

[55] *Montoya de Hernandez*, 473 U.S. at 541.

[56] *Id.* at 550 (Brennan, J., dissenting).

[57] *Montoya de Hernandez*, 473 U.S. at 553; *see also* Das, *supra* note 3, at 220.

ascertain whether a person can legally enter the United States or is carrying contraband. Any more may be an unconstitutional government intrusion on the fundamental right to informational privacy, as discussed herein.

III. SUPREME COURT JURISPRUDENCE HOLDS THAT THE RIGHT TO INFORMATIONAL PRIVACY FOR MOBILE DEVICE DATA IS A FUNDAMENTAL RIGHT UNDER THE DUE PROCESS CLAUSE

The Due Process Clause of the Fifth Amendment states that "[n]o person shall . . . be deprived of life, liberty, or property, without due process of law."[58] Supreme Court jurisprudence dictates that fundamental rights stem from the Due Process Clause.[59] Further, the Court has deemed that fundamental rights require heightened protection from any government intrusion—for example, statutes, regulations, and government agency rules—such that these intrusions are subject to strict scrutiny.[60] That is, the government intrusion must be narrowly tailored to promote a compelling government interest.[61] The Court has held that the constitutional privacy right is a fundamental right[62] and has separated it into two categories: the right to informational privacy and the right to decisional privacy.[63] The right to informational privacy includes the right to control the disclosure of personal information without government interference.[64] The right to decisional privacy includes, among other things, the right to marry, the right to control the upbringing of one's children, and the right to certain private intimate relations.[65] The Supreme Court has held that

---

[58] U.S. CONST. amend. V.

[59] *See, e.g.*, Washington v. Glucksberg, 521 U.S. 702, 720 (1997).

[60] *Id.* at 721; Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1283 (2007) (stating that government intrusion of fundamental rights is subject to strict scrutiny, starting from *Roe v. Wade*).

[61] Fallon, *supra* note 60, at 1284.

[62] Lee Goldman, *The Constitutional Right to Privacy*, 84 DENV. U. L. REV. 601, 602 (2006) (stating "a conceptualization of a central branch of the fundamental rights doctrine [is] the constitutional right to privacy").

[63] Whalen v. Roe, 429 U.S. 589, 598–99 (1977); *see also* Fan, *supra* note 22, at 966 ("From its start, informational privacy was linked to decisional privacy from the common concern of state interference with the autonomy of choice.").

[64] *Whalen*, 429 U.S. at 598–99; *see also* NASA v. Nelson*,* 562 U.S. 134, 138 (2011); Nixon v. Adm'r of Gen. Servs.*,* 433 U.S. 425, 457 (1977).

[65] Washington v. Glucksberg, 521 U.S. 702, 720 (1997); *see also* Fan, *supra* note 22, at 959–66; Goldman, *supra* note 62, at 604–11.

the right to decisional privacy is fundamental.[66] However, the Court has been less clear on whether the right to informational privacy is as well.[67]

Characterizing the right to informational privacy as fundamental would subject any governmental intrusion on one's right of informational privacy to strict scrutiny.[68] Thus, the governmental intrusion must be narrowly tailored to promote a compelling government interest; else, the intrusion is unconstitutional.[69] Using warrantless border searches of United States citizens' mobile device data as an example of a government intrusion on the right to informational privacy, recent Supreme Court case law bolsters the constitutional protection for mobile device data; this thereby elevates the right to informational privacy with regard to mobile device data to a fundamental right, such that a warrantless border search of mobile device data should be subject to strict scrutiny.[70]

Further, a government intrusion can comport with one aspect of the Constitution but violate another.[71] For example, although the warrantless border search of mobile device data may be found to be constitutional under the border search exception doctrine in view of the Fourth Amendment, the warrantless border search of mobile device data can be found to be an unconstitutional government intrusion on the right to informational privacy under the Fifth Amendment.[72] This asymmetry is even more apparent when the constitutional provisions at issue are the search and seizure provisions of the Fourth Amendment and the Due Process Clause of the Fifth

---

[66] Obergefell v. Hodges*,* 135 S. Ct. 2584, 2602 (2015); *see also* Goldman, *supra* note 62, at 604–611; ROTUNDA & NOWAK, *supra* note 1.

[67] *See Whalen*, 429 U.S. at 603–04; *Nelson*, 562 U.S. at 159; *see also* Fan, *supra* note 22, at 968–69.

[68] Fallon, *supra* note 60, at 1269.

[69] *Id.* at 1268.

[70] *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Riley v. California, 573 U.S. 373, 403 (2014) (discussing mobile device data).

[71] Olmstead v. United States*,* 277 U.S. 438, 475 (1928) (Brandeis, J. dissenting) (explaining that an illegal search of a person is not simply a trespass but the "right to be let alone" anywhere). Further, stating that if Fourth Amendment protections are not available, the Fifth Amendment should protect a person's privacy—"[i]n this regard the Fourth and Fifth Amendments run almost into each other." *Id.* (internal quotations omitted). *Olmstead* was eroded to the point that it was overruled by *Katz v. United States,* the case which provides the basis for modern Fourth Amendment jurisprudence with Justice Harlan's reasonable expectation of privacy test. 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring).

[72] *See Olmstead*, 277 U.S. at 475 (Brandeis, J., dissenting).

Amendment; these two rights can overlap such that when one right does not protect a constitutional privacy interest, the other may do so.[73]

The constitutional right to privacy under the Due Process Clause of the Fifth and Fourteenth Amendments can be classified into two categories: (1) the right to informational privacy that involves protecting private personal matters from government intrusion such as medical records and electronic information, and (2) the right to decisional privacy that prevents government interference in personal decision making such as marital decisions, child rearing, and intimate personal relations, each of which the Supreme Court as discussed in several different cases.[74]

A. Supreme Court Jurisprudence Regarding the Right to Informational Privacy and the Right to Decisional Privacy

Regarding the first category, there are three Supreme Court cases that explicitly deal with the constitutional right to informational privacy: *Whalen v. Roe*, *Nixon v. Administrator of General Services*, and *NASA v. Nelson*.[75] The constitutional right to informational privacy can be defined as the right of a person to control the disclosure of his or her personal matters, as articulated in *Whalen*.[76] *Nixon* further cultivated the constitutional right to informational privacy in the context of presidential recordings.[77] Moreover, *Nelson* acknowledged that there is some constitutional protection for personal information but not under the circumstances of that case.[78] However, the Court in *Nelson* was reluctant to clearly state whether the right to informational privacy is a fundamental right, thereby causing confusion on whether strict scrutiny applies to a government intrusion into the right to informational privacy.[79]

---

[73] *Carpenter*, 138 S. Ct. at 2253 (Alito, J., dissenting); *Olmstead*, 277 U.S. at 475 (Brandeis, J., dissenting).

[74] Whalen v. Roe, 429 U.S. 583, 598–600 (1977).

[75] NASA v. Nelson*,* 562 U.S. 134, 138 (2011); *Whalen*, 429 U.S. at 598–600; Nixon v. Adm'r of Gen. Servs*,* 433 U.S. 425, 457 (1977); *see also* Fan, *supra* note 22, at 968–69.

[76] 429 U.S. at 598–600.

[77] *Nixon*, 433 U.S. at 456–57.

[78] *Nelson*, 562 U.S. at 158–59.

[79] Fan, *supra* note 22, at 982; *see also Nelson*, 562 U.S. at 158–59.

The second category, the right to decisional privacy, stems from *Griswold v. Connecticut* and is bolstered by *Obergefell v. Hodges*, along with other cases.[80] This line of cases cements the constitutional right to decisional privacy as fundamental, and any governmental intrusion into this privacy right is subject to strict scrutiny.[81] The right to privacy comprises both the rights to informational privacy and decisional privacy; therefore, if decisional privacy is fundamental and of equal importance to personal liberty as informational privacy, the right to informational privacy should also be regarded as a fundamental right subject to strict scrutiny.[82]

Scholars attribute *Whalen v. Roe* as the Supreme Court's first recognition of the right to informational privacy.[83] Issued in 1977, a few years after the decisional privacy case *Griswold v. Connecticut*, the Court delivered its opinion with the backdrop of recognizing fundamental rights inherent in the Due Process Clauses of the Fifth and Fourteenth Amendments, including both aspects of the constitutional right to privacy.[84]

Whalen considered the New York State Controlled Substances Act, which required disclosing to a government agency the names and addresses of each person who obtained certain drugs through a physician's prescription.[85] The purpose of the law was to track whether certain drugs were being diverted into a black market through corrupt pharmacists refilling prescriptions for unwitting patients.[86] However,

---

[80] Obergefell v. Hodges, 135 S. Ct. 2584, 2602 (2015); Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965); *see* ROTUNDA & NOWAK, *supra* note 1; Goldman, *supra* note 62, at 604–05.

[81] Fallon, *supra* note 60, at 1283.

[82] Fan, *supra* note 22, at 966–67 (stating that informational privacy has always been linked to decisional privacy because they have "the common concern of state interference with autonomy of choice"); see *also* Fallon, *supra* note 60, at 1283. Professor Fan also quotes District Court Judge Robert L. Carter, who stated:

> The concept of privacy is an affirmation of the importance of certain aspects of the individual and his desired freedom from needless outside interference. It is sometimes described as a sphere of space that a man may carry with him which is protected from unwarranted outside intrusion, as the right of selected disclosures about oneself and as a right of personal autonomy.

Fan, *supra* note 22, at 966–67.

[83] 429 U.S. 589, 591 (1977); *see also* Fan, *supra* note 22, at 955.

[84] Griswold v. Connecticut, 381 U.S. 479, 485 (1965); *Whalen*, 429 U.S. at 598–99; *see also* Roe v. Wade, 410 U.S. 113, 153–54 (1973).

[85] *Whalen*, 429 U.S. at 591.

[86] *Id.* at 591–92.

patients believed that disclosure of their names, even though only to a government agency, would be damaging to their reputation by stigmatizing them as drug addicts.[87] A group of patients challenged the statute as a violation of their "constitutionally protected rights of privacy."[88]

Justice Stevens delivered the majority opinion and found that there are two different kinds of privacy interests provided by the Constitution.[89] Specifically, he stated that "[o]ne is the individual interest in avoiding disclosure of personal matters," construed as the right to informational privacy, "and another is the interest in independence in making certain kinds of important decisions," construed as the right to decisional privacy.[90] Further, the Court found that the right to informational privacy is protected by the Fourteenth Amendment.[91] Moreover, the Court enacted a balancing test between the health of the community to prevent prescription drugs from falling into the black market and the patients' right to informational privacy.[92] After balancing the benefits of the statute with the invasion on the patients' privacy rights, the Court held that the statute's disclosure requirements did not constitute an impermissible invasion on "any right or liberty protected by the Fourteenth Amendment."[93]

Justice Stevens cited Justice Brandeis's dissent in *Olmstead v. United States* in stating that there is a right to informational privacy.[94] *Olmstead* was a telephone wiretapping case in which the Court held there is no violation of the Fourth Amendment where law enforcement does not trespass on a person's property.[95] Justice Brandeis emphatically stated that the Constitution provides the "right to be let alone," or to be free from government intrusion.[96] Seizing on this language, the Court in *Whalen* established the right to informational privacy.[97]

---

[87] *Id.* at 595.
[88] *Id.* at 591.
[89] *Id.* at 599–600.
[90] *Id.* at 599–600.
[91] *Id.* at 603–04.
[92] *Id.* at 602.
[93] *Id.* at 603–04.
[94] *Id.* at 599 n.25 (citing Olmstead v. United States, 277 U.S. 438, 475 (1928) (Brandeis, J. dissenting)).
[95] *Olmstead*, 277 U.S. at 468.
[96] *Id.* at 478.
[97] *Whalen*, 429 U.S. at 599*; see supra* note 71 (discussing that *Olmstead* was eroded over decades and overturned by *Katz*).

In his concurrence in *Whalen*, Justice Brennan stated that the statute discloses patients' personal information to only a small number of state health officials with a legitimate interest in the information.[98] However, Justice Brennan argued that disclosure to a wide array of people "would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests."[99] The use of "compelling state interest" language implies that the right to informational privacy is subject to strict scrutiny.[100] Thus, the majority opinion set the precedent by establishing the constitutional right to informational privacy, and Justice Brennan further stated that the right to informational privacy is subject to strict scrutiny, implicitly establishing the right to informational privacy as fundamental, like its decisional privacy counterpart.[101]

In *Nixon v. Administrator of General Services*, decided a few months after *Whalen*, the Court dealt with releasing President Nixon's recordings that were made during his presidency.[102] Justice Brennan delivered the opinion of the Court regarding whether the release of the recordings violated President Nixon's constitutional privacy interests.[103] President Nixon was compelled to release the recordings to the Administrator of General Services under the Presidential Recordings and Materials Preservation Act ("Act").[104] Further, the Administrator was to screen the recordings for personal information regarding the President and only release recordings that were pertinent to the public.[105] In light of this screening process, Justice Brennan found that President Nixon's privacy interest in his personal communications was outweighed by the compelling state interest in having recordings pertinent to the public be released using the the strict scrutiny rubric.[106] That is, Justice Brennan stated that the Act's screening process was narrowly tailored to achieve the compelling state interest and that it attempted to keep President

---

[98] *Whalen*, 429 U.S. at 606 (Brennan, J., concurring).
[99] *Id.*
[100] *See id.* at 606–07.
[101] *Id.* at 603–04 (majority opinion), 606 (Brennan, J., concurring).
[102] 433 U.S. 425, 429 (1977).
[103] *Id.*
[104] *Id.* at 433.
[105] *Id.* at 455, 463.
[106] *Id.* at 465.

Nixon's personal recordings private.[107] Thus, Justice Brennan further cemented the right to informational privacy and its status as a fundamental right subject to strict scrutiny.[108] Any government intrusion on the right to informational privacy, therefore, must be narrowly tailored to achieve a compelling government interest.[109]

In *NASA v. Nelson*, contract employees sued NASA for requiring a background check for employment, alleging that it invaded their constitutional right to informational privacy.[110] Justice Alito, in delivering the opinion for the Court, was reluctant to acknowledge a constitutional right to informational privacy, stating "we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance."[111] Further, Justice Alito found that the Government did not have the "constitutional burden to demonstrate that its questions are 'necessary' or the least restrictive means of furthering its interests."[112] Instead, Justice Alito enacted a less exacting balancing test, weighing the Government's interest in employing reliable workers that perform functions critical to NASA's mission against the workers' right of informational privacy.[113] As a result, the Court held, based on this balancing test, that the Government's background check did not violate the contract employees' right to informational privacy.[114] Thus, *Nelson* established that the right to informational privacy may be subject to less than strict scrutiny.[115]

However, as described herein, there are two further reasons the right to informational privacy should be a fundamental right, the government intrusion of which should be subject to strict scrutiny. First, the right to decisional privacy is equal in constitutional importance to the right to informational privacy, and if decisional privacy is a fundamental right, so must be informational privacy.[116] Second, recent Supreme Court

---

[107] *Id.* at 456–57.
[108] *See id.* at 456–57, 465.
[109] *See id.*
[110] 562 U.S. 134, 138 (2011).
[111] *Id.* at 147.
[112] *Id.* at 153.
[113] *See id.* at 150–51.
[114] *Id.* at 159.
[115] *See id.* at 150.
[116] *See* Fan, *supra* note 22, at 966–67.

decisions regarding constitutional privacy protections of mobile device data can be construed to elevate the right to informational privacy to a fundamental right, such that any government intrusion is subject to strict scrutiny.[117]

Discussions of decisional privacy led to *Griswold v. Connecticut*, in which individuals challenged a Connecticut statute that made it a crime for a physician to provide contraceptives, even to married couples.[118] Justice Douglas, writing for the Court, found that the Fourth, Fifth, and Ninth Amendments provided a constitutional right to privacy to protect governmental intrusion into a person's private decisions.[119] Further, the Court subjected the statute to strict scrutiny in view of its violation of the constitutional right to decisional privacy.[120] The Court found that the statue swept "unnecessarily broadly" to "control or prevent [contraceptive] activities."[121] Justice Harlan, in his concurrence, adhered the notion that the decisional privacy right to contraception is a fundamental right by stating that the Connecticut statute violated the Due Process Clause of the Fourteenth Amendment.[122]

In *Obergefell v. Hodges*, same-sex couples were given the right to marry.[123] The Supreme Court case consolidated cases from Michigan, Kentucky, Ohio, and Tennessee.[124] Justice Kennedy delivered the opinion of the Court and found that "[o]ver time and in other contexts, the Court has reiterated that the right to marry is fundamental under the Due Process Clause."[125] Further, Justice Kennedy stated that "the reasons marriage is fundamental under the Constitution apply with equal force to same-sex couples."[126] In addition, the Court held "there is no lawful basis for a State to refuse to recognize a lawful same-sex marriage."[127] Finally, Justice Kennedy stated

---

[117] Carpenter v. United States*,* 138 S. Ct. 2206, 2223 (2018); Riley v. California, 573 U.S. 373, 403 (2014).

[118] Griswold v. Connecticut*,* 381 U.S. 479, 480 (1965).

[119] *Id.* at 484–85.

[120] *Id.* at 485.

[121] *Id.*

[122] *Id.* at 500 (Harlan, J., concurring).

[123] 135 S. Ct. 2584, 2608 (2015).

[124] *Id.* at 2593.

[125] *Id.* at 2598.

[126] *Id.* at 2599.

[127] *Id.* at 2608.

> It would misunderstand these men and women to say they disrespect the idea of marriage. Their plea is that they do respect it, respect it so deeply that they seek to find its fulfillment for themselves. Their hope is not to be condemned to live in loneliness, excluded from one of civilization's oldest institutions. They ask for equal dignity in the eyes of the law. The Constitution grants them that right.[128]

There are other Supreme Court cases that establish the right to decisional privacy as a fundamental right subject to strict scrutiny.[129] Further, Justice Stevens and Justice Brennan in *Whalen* established that the right to informational privacy is as constitutionally important as the right to decisional privacy.[130] The confusion in the current judicial landscape stems from Justice Alito's application of a scrutiny less than strict in *Nelson* without distinguishing it from *Whalen* and *Nixon*.[131] However, as described herein, Justice Alito's view of the right to informational privacy contravenes previous Supreme Court jurisprudence.[132] Moreover, recent Supreme Court case law provides clarity by holding that mobile device data requires heightened constitutional protection, likely elevating the right to informational privacy with regard to mobile device data to a fundamental right.[133]

B. Recent Supreme Court Cases Regarding the Constitutional Privacy Protections of Mobile Device Data Bolster Right to Informational Privacy as Fundamental Right

Although there has been no specific Supreme Court case dealing with the constitutional right to informational privacy with regard to mobile device data, the Supreme Court has dealt with the warrantless search of mobile devices, albeit not at the border.[134] In *Riley v. California*, David Leon Riley was stopped by the police while driving his vehicle with expired registration

---

[128] *Id.*

[129] *See* ROTUNDA & NOWAK, *supra* note 1.

[130] Whalen v. Roe, 429 U.S. 589, 603–04 (majority opinion), 606 (Brennan, J., concurring) (1977).

[131] NASA v. Nelson, 562 U.S. 134, 150 (2011); *Whalen*, 429 U.S. at 607 (Brennan, J., concurring).

[132] *Whalen*, 429 U.S. at 607 (Brennan, J., concurring); *see also* Fan, *supra* note 22, at 966–67.

[133] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Riley v. California, 573 U.S. 373, 403 (2014).

[134] *Carpenter,* 138 S. Ct. at 2223; *Riley*, 573 U.S. at 403.

tags.[135] During the traffic stop, the police found that Riley was driving under a suspended license.[136] As a matter of standard operating procedure, the police impounded Riley's vehicle.[137] During an inventory search of the vehicle, police found two concealed firearms that led to Riley's arrest for being in possession of them.[138] Upon a warrantless search of Riley's person incident to arrest, the police seized a mobile phone and personal effects that indicated Riley's gang affiliation.[139] The police continued searching the contents of the mobile phone and found photographs of Riley in front of a car that was involved in a shooting a few weeks earlier.[140] Riley was charged with the earlier shooting based at least in part due to the evidence found from the search of his mobile phone.[141] Riley moved to suppress the evidence found on his mobile phone on the basis that it was found through a warrantless search.[142] The trial court denied the motion, and the California Court of Appeal affirmed.[143]

Chief Justice Roberts issued the majority opinion that stated, based on Supreme Court precedent, that the purpose of a warrantless search incident to arrest is to remove any weapons that pose a threat to law enforcement and to prevent the destruction of evidence.[144] Further, Chief Justice Roberts stated that "we generally determine whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.' "[145] Thus, the Court subjected the government intrusion of a warrantless search of mobile device data incident to an arrest to heightened scrutiny.[146]

In addition, the Court addressed the basis for the search incident to arrest exception by stating "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting

---

[135] *Riley,* 573 U.S. at 378.
[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.* at 378–79.
[140] *Id.* at 379.
[141] *Id.* at 379–80.
[142] *Id.*
[143] *Id.*
[144] *Id.* at 381–83.
[145] *Id.* at 385 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
[146] Fallon, *supra* note 60, at 1283; *see also Riley*, 573 U.S. at 385–86.

officer or to effectuate the arrestee's escape."[147] Further, the Court found that law enforcement officers can conduct a warrantless search of a mobile phone to determine that no weapons are hidden within it.[148] However, once it is determined that the mobile phone is not hiding any weapons, there is no need to conduct a warrantless search of the data on the mobile phone to ensure officer safety.[149] Further, Chief Justice Roberts addressed the other aspect of the search incident to arrest doctrine by stating that "once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone."[150]

Thus, the underlying rationale of the search incident to arrest doctrine is to allow a warrantless search incident to an arrest to find weapons in order to protect law enforcement officers and to prevent the destruction of evidence.[151] The Court held in *Riley* that any further search, including a search of the data accessible via a mobile phone, requires a search warrant based on probable cause because a mobile phone is not simply a communication device but can contain the most intimate details of a person's life.[152] These kinds of intimate details are ones that require heightened constitutional protection.[153]

In *Carpenter v. United States*, law enforcement officials were gathering location information for Carpenter, which was provided by his mobile phone to cell towers in Michigan and Ohio.[154] Using the location information collected, without a warrant, from the cell phone carrier, law enforcement officers were able to place Carpenter at several robberies.[155] Carpenter moved to suppress the location information as a violation of his reasonable expectation of privacy under the Fourth Amendment.[156]

---

[147] *Riley*, 573 U.S. at 387.

[148] *Id.* ("to determine whether there is a razor blade hidden between the phone and its case").

[149] *Id.*

[150] *Id.* at 388.

[151] *Id.* at 386–88.

[152] *Id.* at 388, 401–03.

[153] *Id.*

[154] 138 S. Ct. 2206, 2212 (2018).

[155] *Id.*

[156] *Id.*

Chief Justice Roberts delivered the opinion of the Court, holding that although Carpenter provided his location information to the third-party cell phone carrier, such location information was so integral to ascertaining his constant whereabouts that he had a reasonable expectation of privacy in his location information under the Fourth Amendment.[157] Thus, law enforcement officers were required to obtain a warrant prior to gathering the location information regarding Carpenter's cell phone from the cell phone carrier.[158]

The Court found that because location information of a mobile device is so intimate, it requires heightened constitutional protection.[159] Although, as in *Riley*, *Carpenter* implicates the Fourth Amendment, the Court, citing Justice Brandeis's dissent from *Olmstead*, found that an individual's privacy in his mobile device data—particularly location information—should not be eroded through technological advances in government surveillance.[160] Further, Chief Justice Roberts cited Justice Brandeis's dissent from *Olmstead* to find that a person has the "right to be let alone" from government intrusion, further justifying mobile device data as meriting heightened constitutional protection from government intrusion.[161]

In the context of searches incident to arrest, the Court has held that the Fourth Amendment requires a warrant prior to searching mobile device data.[162] However, in the context of a border search, the Court has not yet opined on whether the Fourth Amendment provides constitutional protections from a warrantless government search of mobile device data at the border.[163] Further, lower courts have held that the border search exception allows law enforcement to search mobile device data without obtaining a warrant.[164]

Allowing a warrantless border search of mobile device data contravenes the constitutional protections of mobile device data found in both *Riley* and *Carpenter*.[165] If the Fourth Amendment

---

[157] *Id.* at 2221–22.
[158] *Id.* at 2221.
[159] *Id.* at 2217
[160] *Id.* at 2223.
[161] *Id.* (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J. dissenting)).
[162] Riley v. California, 573 U.S. 373, 403 (2014).
[163] Miller, *supra* note 5, at 1963.
[164] *Id.* at 1982–83.
[165] *See* Das, *supra* note 3, at 239.

is not capable of providing these constitutional protections, then the Fifth Amendment may be.[166] That is, although a warrantless border search of mobile device data may be constitutional under the Fourth Amendment, the same warrantless border search can infringe on the right to informational privacy.[167] Such a rationale is in line with Justice Roberts's rationale and citation to Justice Brandeis's dissent in *Olmstead*, which is the same line of jurisprudence from which the right of informational privacy was born.[168]

C. The Right to Informational Privacy for Mobile Device Data is a Fundamental Right Requiring Strict Scrutiny

Any government intrusion of the fundamental right to informational privacy is subject to strict scrutiny for three reasons. First, the right to informational privacy is of equal constitutional importance to the right to decisional privacy.[169] Thus, if the Supreme Court jurisprudence finds that decisional privacy is a fundamental right, it follows that informational privacy is also a fundamental right.[170] Second, the recent Supreme Court cases *Riley* and *Carpenter* have found that mobile device data receives heightened constitutional privacy protection.[171] Third, the *Carpenter* rationale for requiring heightened protection for mobile device data stems from the same Supreme Court jurisprudence as the right to informational privacy.[172] Therefore, if mobile device data requires heightened constitutional protection and the right to informational privacy covers mobile device data, then the right to privacy vis-à-vis mobile device data is a fundamental right.[173]

Supreme Court jurisprudence for the right to informational privacy—found in cases from *Whalen* through *Nixon* to *Nelson*—has vacillated between strict scrutiny and something

---

[166] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); *Olmstead*, 277 U.S. at 475.

[167] *Carpenter*, 138 S. Ct at 2223; *Olmstead*, 277 U.S. at 474–76.

[168] *Carpenter*, 138 S. Ct at 2223; *Olmstead*, 277 U.S. at 474–76.

[169] *See* Fan, *supra* note 22, at 966–67; *see also* Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J., concurring).

[170] *Whalen*, 429 U.S. at 607 (Brennan, J., concurring).

[171] *Carpenter*, 138 S. Ct at 2223; Riley v. California, 573 U.S. 373, 403 (2014).

[172] *Carpenter*, 138 S. Ct. at 2223 (citing Olmstead v. United States, 277 U.S. 438, 475 (1928) (Brandeis, J. dissenting)).

[173] Obergefell v. Hodges, 135 S. Ct. 2584, 2593 (2015); *Whalen*, 429 U.S. at 607 (Brennan, J., concurring); Fan, *supra* note 22, at 966–67.

less, thereby creating confusion about whether informational privacy is a fundamental right protected by the Due Process Clause of the Fifth and Fourteenth Amendments.[174] However, the right to decisional privacy, akin to the right to informational privacy, enjoys the status of a fundamental right[175] Supreme Court jurisprudence relating to the right to decisional privacy starts with *Griswold v. Connecticut* and continues through *Roe v. Wade* and *Obergefell v. Hodges*, among others.[176] This line of cases establishes that any government intrusion on the constitutional right to decisional privacy must be subject to strict scrutiny.[177] The right of informational privacy is likely of equal constitutional importance as the right to decisional privacy because they stem from the same concern by the Supreme Court about state interference in an invidual's right to make choices about her own life.[178] Thus, like the right to decisional privacy, the right to informational privacy should be considered a fundamental right, any government intrusion of which is subject to strict scrutiny.[179]

Moreover, the recent Supreme Court cases *Riley* and *Carpenter* hold that mobile device data can store such intimate details of a person's life that it requires constitutional protection from government intrusion.[180] While both *Riley* and *Carpenter* consider mobile device data through a Fourth Amendment lens, the Supreme Court has held in both cases that mobile device data requires heightened constitutional protection based on the ubiquity of cell phones in daily life.[181]

---

[174] NASA v. Nelson*,* 562 U.S. 134, 138 (2011); *Whalen*, 429 U.S. at 598–99; Nixon v. Adm'r of Gen. Servs*,* 433 U.S. 425, 457 (1977).

[175] *Obergefell*, 135 S. Ct. at 2602; Roe v. Wade, 410 U.S. 113, 154 (1973); Griswold v. Connecticut, 381 U.S. 479 (1965); *see also* Goldman, *supra* note 62, at 602; ROTUNDA & NOWAK, *supra* note 1. *Roe* established the right to decide whether to have an abortion as a fundamental right, but after *Casey*, this right is no longer considered to be fundamental.

[176] *Obergefell*, 135 S. Ct. at 2602*; see also* Goldman, *supra* note 62, at 602; ROTUNDA & NOWAK, *supra* note 1.

[177] *Obergefell*, 135 S. Ct. at 2602*; see* Fallon, *supra* note 60, at 1284; Goldman, *supra* note 62, at 602.

[178] Fan, *supra* note 22, at 967–69.

[179] *Whalen*, 429 U.S. at 607 (Brennan, J., concurring); *see also* Fan, *supra* note 22, at 968–69.

[180] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Riley v. California, 573 U.S. 373, 403 (2014).

[181] *Carpenter*, 138 S. Ct. at 2223; *Riley*, 573 U.S. at 403.

Further, Chief Justice Roberts, in *Carpenter*, noted that constitutional privacy protection for mobile device data has its roots in Justice Brandeis's dissent in *Olmstead*, as did Justice Stevens in *Whalen*, when he recognized the constitutional right to informational privacy.[182] Justice Brandeis wrote that the Constitution provides the "right to be let alone" stemming from the Fifth Amendment.[183] Further, Justice Brandeis explained that personal privacy and personal liberty are so intertwined that "the Fourth and Fifth Amendments run almost into each other."[184] The portion of Justice Brandeis's dissent in *Olmstead* that Chief Justice Roberts cited to lay the foundation for mobile device data's heightened protection is the same portion that provided the basis for informational privacy.[185] Therefore, the right to informational privacy for mobile device data should be recognized as a fundamental right requiring heightened constitutional protection.[186]

IV. RECENT SUPREME COURT RULINGS SHOULD ASSUAGE SOME LEGAL COMMENTATORS' RELUCTANCE TO FIND THAT A GOVERNMENT INTRUSION ON THE RIGHT TO INFORMATIONAL PRIVACY IS SUBJECT TO STRICT SCRUTINY

After *Nelson*, some legal commentators questioned whether the right to informational privacy is a fundamental right.[187] Further, some legal commentators questioned whether there is a constitutional right to privacy at all due to Justice Scalia's and Justice Thomas's concurrences in that case, which deny that such a right is protected by the Constitution.[188] However, other legal scholars do accept that the Constitution provides a right to

---

[182] *Carpenter*, 138 S. Ct. at 2223; Olmstead v. United States*,* 277 U.S. 438, 475 (1928) (Brandeis, J. dissenting).

[183] *Olmstead*, 277 U.S. at 478.

[184] *Id.* at 475.

[185] *Carpenter*, 138 S. Ct at 2223.

[186] *Carpenter*, 138 S. Ct. at 2223; *Riley*, 573 U.S. at 403; *Whalen*, 429 U.S. at 607 (Brennan, J., concurring); *see also* Fan, *supra* note 22, at 968–69.

[187] Fan, *supra* note 22, at 968–69; Caleb A. Seeley, Note, *Once More Unto the Breach: The Constitutional Right to Informational Privacy and the Privacy Act*, 91 N.Y.U. L. REV. 1355, 1360–62 (2016); Blythe Golay, Comment, NASA v. Nelson*: The High Court Flying High Above the Right to Informational Privacy*, 45 LOY. L.A. L. REV. 477, 478 (2012); Russell T. Gorkin, *The Constitutional Right to Informational Privacy:* NASA v. Nelson, 6 DUKE J. CONST. L. & PUB. POL'Y SIDEBAR 1, 1–2 (2010).

[188] NASA v. Nelson, 562 U.S. 134, 160 (Scalia, J., concurring), 169 (Thomas, J., concurring) (2011); *see also* Fan, *supra* note 22, at 982; Gorkin, *supra* note 187, at 6; Golay, *supra* note 187, at 483.

informational privacy, but they find that any government intrusion of such a right is not subject to strict scrutiny and instead, they put forth that a right to informational privacy is subject to some form of intermediate scrutiny.[189]

An oft-cited argument that a right to informational privacy does not exist is the cliché that there is no such explicit right stated in the Constitution.[190] However, this belief is hypocritical at best, as the Court has recognized time and again that the right to decisional privacy—akin to the right to informational privacy—is also not explicitly stated in the Constitution, but is a fundamental right nonetheless.[191] Another reason for the reluctance to acknowledge the right to informational privacy is the existence of only three Supreme Court cases on the issue: *Whalen*, *Nixon*, and *Nelson*.[192] A further reason for reluctance is that in each of those three cases, the party asserting the right failed to vindicate the right because of a compelling government interest.[193] Moreover, these three cases apply varying levels of scrutiny, ranging from strict scrutiny to a simple balancing test of a person's interest against the government's interest.[194]

However, given federal jurisprudence with regard to the right to informational privacy and the recent Supreme Court cases with regard to mobile device data, legal commentators should be more willing to accept that the right to informational privacy for mobile device data is a fundamental right.[195] Lower federal courts have continued to hold that a right to informational privacy exists, and the Supreme Court has refused to grant certiorari in any of these cases, which may implicitly acknowledge that a right to informational privacy exists.[196] These cases range from enjoining the Department of Defense and the Department of Housing and Urban Development from asking

---

[189] *See Seeley*, *supra* note 187, at 1361; Gorkin, *supra* note 187, at 20; Fan, *supra* note 22, at 981.

[190] *Nelson*, 562 U.S. at 160 (Scalia, J., concurring), 169 (Thomas, J., concurring); *see also* Fan, *supra* note 22, at 982; Gorkin, *supra* note 187, at 6; Golay, *supra* note 187, at 483.

[191] *Obergefell*, 135 S. Ct. at 2602; *see also* ROTUNDA & NOWAK, *supra* note 1.

[192] Fan, *supra* note 22, at 954–55; *see also* Gorkin, *supra* note 187, at 20; Golay, *supra* note 187, at 478; Seeley, *supra* note 187, at 1362.

[193] *Nelson*, 562 U.S. at 138 (2011); Whalen v. Roe, 429 U.S. 589, 598-99 (1977); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977).

[194] *Nelson*, 562 U.S. at 153, 159; *Whalen*, 429 U.S. at 605–07; *Nixon*, 433 U.S. at 464–65.

[195] Fan, *supra* note 22, at 988; *see also* Gorkin, *supra* note 187, at 20.

[196] Fan, *supra* note 22, at 981.

employees about their drug use and financial history to preventing the revelation of the HIV status of prison inmates or the personal details of rape victims.[197] This all suggests that the lower federal courts find that some sort of right to informational privacy exists.[198]

Further, legal commentators should analyze the Supreme Court cases directly addressing the right to informational privacy, not in a vacuum, but against the backdrop of other relevant Supreme Court cases.[199] *Riley* and *Carpenter* have found heightened constitutional protection of mobile device data.[200] In *Riley*, the Court found that mobile devices store and have access to the most intimate details of a person's life, such that law enforcement officers cannot freely search their contents without a warrant.[201] In *Carpenter*, the Court again found that location information of a mobile device contains intimate details of a person's life.[202] A mobile device, such as a mobile phone, is in a person's possession constantly in his everyday life. Thus, the location information of a mobile device is the location information of the person.[203] Such intimate details are held to be constitutionally protected from law enforcement officers who wish to freely search the phone's contents without a warrant.[204]

In addition, *Riley* and *Carpenter* both found that mobile device data contains the most private details of a person's life.[205] Thus, the Court held in both *Riley* and *Carpenter* that any search of mobile device data requires a warrant.[206] In Supreme Court jurisprudence, where the Fourth Amendment falls short, the Fifth Amendment can protect the right.[207] The Court found in both *Riley* and *Carpenter* that mobile device data is afforded heightened constitutional protection; therefore, cell phone data

---

[197] *Id.* at 973–74, 977–79, 985–86.

[198] *Id.*

[199] Carpenter v. United States. 138 S. Ct. 2206, 2223 (2018); Riley v. California, 573 U.S. 373, 403 (2014).

[200] *Carpenter*, 138 S. Ct. at 2223; *Riley*, 573 U.S. at 403.

[201] *Riley*, 573 U.S. at 403.

[202] *Carpenter*, 138 S. Ct. at 2218.

[203] *Id.*

[204] *Id.*

[205] *Carpenter*, 138 S. Ct. at 2218; *Riley*, 573 U.S. at 403.

[206] *Carpenter*, 138 S. Ct. at 2223; *Riley*, 573 U.S. at 403.

[207] Fallon, *supra* note 60, at 1283; *see also* ROTUNDA & NOWAK, *supra* note 1, at § 15.7.

falls under the protection of the informational privacy right, and any government intrusion on this constitutionally protected privacy interest must be subject to strict scrutiny.[208]

Thus, with lower federal courts acknowledging the right to informational privacy and the Supreme Court implying as such, in addition to the recent Supreme Court cases holding that mobile device data merits heightened constitutional protection, legal commentators should find that the right to informational privacy, at least as it pertains to mobile device data, is a fundamental right, any government intrusion of which must be subject to strict scrutiny.[209]

V. DHS RULES CALLING FOR WARRANTLESS BORDER SEARCH OF MOBILE DEVICE DATA ARE UNCONSTITUTIONAL FOR VIOLATING THE RIGHT TO INFORMATIONAL PRIVACY

As discussed herein, the right to informational privacy, at least as it pertains to mobile device data, is a fundamental right, and any government intrusion on it should be subject to strict scrutiny.[210] That is, the government intrusion must be narrowly tailored to serve a compelling government interest.[211]

DHS rules that allegedly allow CBP officials to conduct a warrantless border search of mobile device data can be construed as a government intrusion on the right to informational privacy for mobile device data.[212] The compelling government interest for such a government intrusion, as indicated by the DHS rules, is national security, specifically protecting the country from terrorists.[213] The DHS empowers CBP officials to search a United States citizen's mobile device data without a warrant at the border to ferret out terrorists.[214] The rationale is that searching emails, social media, and other electronic data stored on, or accessible from, a person's mobile device would indicate

---

[208] *See Carpenter*, 138 S. Ct. at 2218; *see also Riley*, 573 U.S. at 403.

[209] Fan, *supra* note 22, at 981; *see also Carpenter,* 138 S. Ct. at 2223; *Riley*, 573 U.S. at 403.

[210] Fan, *supra* note 22, at 981; *see also Carpenter,* 138 S. Ct. at 2223; *Riley*, 573 U.S. at 403.

[211] Fan, *supra* note 22, at 981.

[212] *Inspection of Electronic Devices*, *supra* note 4; *Carpenter,* 138 S. Ct. at 2223; *Riley*, 573 U.S. at 40; *see also* Fan, *supra* note 22, at 981.

[213] *Inspection of Electronic Devices*, *supra* note 4; *see also* Motion to Dismiss at 16–18, Alasaad v. Nielsen, 2018 WL 2170323 (D. Mass. May 9, 2018 (No. 17-cv-11730-DJC) [hereinafter Alasaad Motion to Dismiss].

[214] *Inspection of Electronic Devices*, *supra* note 4; *see also* Alasaad Motion to Dismiss, *supra* note 213, at 2.

whether the person has a terrorist ideology.[215] There is no doubt that national security, including identifying terrorists entering our country, is a compelling government interest.[216]

However, such a government intrusion should be subject to strict scrutiny that it is narrowly tailored to the compelling government interest.[217] Unfettered access to and search of mobile device data is not a narrowly tailored government intrusion.[218] Such a government intrusion leaves a United States citizen's constitutionally protected right to informational privacy at the whim of CBP officials, a situation that can lead to tyranny, as suggested by Justice Brennan in his dissent in *Montoya de Hernandez*.[219] Further, such an overbroad government intrusion chills the freedom of speech, as citizens will be less likely to speak out against the government in their emails or social media if they know that CBP officials have unfettered access to this mobile device data every time they reenter the country from abroad.[220] This chilling of political speech is against the nation's founding values.[221]

Thus, warrantless border searches of mobile device data must be narrowly tailored to stave off government tyranny and refrain from chilling political speech.[222] One way to narrowly tailor the warrantless border search of mobile device data and

---

[215] *Inspection of Electronic Devices*, *supra* note 4; *see also* Alasaad Motion to Dismiss, *supra* note 213, at 2.

[216] *See Inspection of Electronic Devices*, *supra* note 4 (describing the government's interest); *see also* Alasaad Motion to Dismiss, *supra* note 213, at 2.

[217] *See Carpenter,* 138 S. Ct. at 2223; *see also Riley*, 573 U.S. at 403; Fan, *supra* note 22, at 981.

[218] United States v. Montoya de Hernandez, 473 U.S. 531, 552 (1985) (Brennan, J., dissenting).

[219] *Id.*

[220] Brief of the Knight First Amendment Institute At Columbia University and The Reporters Committee for Freedom of the Press as *Amici Curiae* Supporting Plaintiffs, Alasaad v. Nielsen, 2018 WL 2170323 (D. Mass. May 9, 2018) (No. 17 Civ. 11730 (DJC)) [hereinafter The Brief]; Amna Toor, Note & Comment*, "Our Identity Is Often What's Triggering Surveillance": How Government Surveillance of #BLACKLIVESMATTER Violates the First Amendment Freedom of Association*, 44 RUTGERS COMPUTER & TECH. L. J. 286, 288 (2018) (explaining that there is a fundamental right of people expressing themselves through their political speech). In this day and age, people use social media to express their political speech. Social media is accessible through mobile devices such as mobile phones and people engage in political speech through their mobile phones. Warrantless search of mobile phones would chill this type of political speech.

[221] The Brief, *supra* note 220; Toor, *supra* note 220, at 291–92.

[222] Whalen v. Roe, 429 U.S. 589, 607 (1977); *Montoya de Hernandez,* 473 U.S. at 552.

cure the unconstitutional government intrusion is to simply require CBP officials to obtain a warrant prior to conducting a border search of mobile device data.[223] Having an independent magistrate decide, *a priori*, whether the border search is constitutional inherently restricts the number of persons whose mobile device data is subject to a border search, thereby narrowly tailoring the government intrusion of warrantless border searches of mobile device data.[224] Moreover, a warrant must be based on probable cause.[225] Therefore, CBP officials would not be able to conduct border searches of mobile device data of persons that they only reasonably suspect or have no reason to suspect to pose a national security risk, but only those that they have probable cause to suspect to be a terrorist.[226] Hence, the pool of potential persons subject to a border search would shrink, thereby narrowly tailoring the government intrusion of a border search.[227]

CONCLUSION

DHS rules have been promulgated to allow CBP officials to conduct warrantless searches of mobile device data at the border of United States citizens returning to the country under the border search exception doctrine of the Fourth Amendment. Such a warrantless border search likely violates the fundamental right to informational privacy for mobile device data, as the right to informational privacy for mobile device data is a fundamental right for three reasons. First, the right to informational privacy is akin to the right to decisional privacy, which has been established as a longstanding fundamental right by Supreme Court jurisprudence. Moreover, the right to informational privacy for mobile device data is of equal importance as the right to decisional privacy. Thus, if the right to decisional privacy is a fundamental right, then logic follows that the right to informational privacy is also a fundamental right. Second, recent Supreme Court cases have held that mobile device data should be subject to heightened constitutional protection. Third, the Supreme Court's rationale for holding mobile device data to require heightened constitutional protection stems from the same

---

[223] *Montoya de Hernandez,* 473 U.S. at 552.
[224] *See id.* at 552.
[225] *Id.* at 553.
[226] *Id.* at 554.
[227] Fallon, *supra* note 60, at 1271–72.

Supreme Court jurisprudence that produced the right of informational privacy. Therefore, if mobile device data requires a heightened level of constitutional protection and the right to informational privacy includes mobile device data, then the right to informational privacy for mobile device data should also be considered fundamental.

Consequently, if the right to informational privacy for mobile device data is deemed to be a fundamental right, then any government intrusion on that right is subject to strict scrutiny. That is, the government intrusion must be narrowly tailored to serve a compelling government interest. Analyzing warrantless border searches of mobile device data under this judicial rubric, the compelling government interest relating to warrantless border searches is national security. That is, CBP officials search mobile device data to ferret out terrorists. The hope is that searching mobile device data reveals a person's terrorist ideology through the search of emails, social media profiles, and more. However, a warrantless border search of mobile device data is not the most narrowly tailored government intrusion on this compelling government interest. Instead, obtaining a search warrant based on probable cause from an independent judicial officer would be more narrowly tailored. Requiring a search warrant provides a mechanism to avoid the potential of searching any and all United States citizens' mobile device data and focuses the border search of mobile device data of United States citizens that CBP officials have probable cause to believe may have a terrorist ideology. Otherwise, the warrantless border search of mobile device data of potentially all United States citizens would chill political speech through a tyrannical invasion of constitutionally protected privacy interests because of its overbroad government intrusion.