

6-21-2019

Chilling Social Media: Warrantless Border Searches of Social Media Accounts Infringe Upon the Freedom of Association and the Freedom to be Anonymous Under the First Amendment

Atanu Das

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/blr>



Part of the [Internet Law Commons](#), and the [Law and Politics Commons](#)

Recommended Citation

Atanu Das, *Chilling Social Media: Warrantless Border Searches of Social Media Accounts Infringe Upon the Freedom of Association and the Freedom to be Anonymous Under the First Amendment*, 84 Brook. L. Rev. (2019).

Available at: <https://brooklynworks.brooklaw.edu/blr/vol84/iss4/5>

This Article is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Law Review by an authorized editor of BrooklynWorks.

Chilling Social Media

WARRANTLESS BORDER SEARCHES OF SOCIAL MEDIA ACCOUNTS INFRINGE UPON THE FREEDOM OF ASSOCIATION AND THE FREEDOM TO BE ANONYMOUS UNDER THE FIRST AMENDMENT

Atanu Das[†]

INTRODUCTION

In its landmark case, *NAACP v. Alabama*, the U.S. Supreme Court held that a person has the freedom of association under the First Amendment.¹ That is, a person can associate with any group without government interference, intrusion, or

© Atanu Das, 2019. The author has not granted rights to reprint this article under a Creative Commons Attribution-Non-Commercial 4.0 License. Please contact the author directly for reprint permission.

[†] Distinguished Scholar, Loyola University Chicago, School of Law. The views in this essay are the author's own. A special thank you to Dean Michael Kaufman, Professor Barry Sullivan, Professor Spencer Waller, Professor Sacha Coupet, and Professor John Breen for their expertise, insight, and encouragement with regard to this essay. Also, I am grateful to my Research Assistants, Dhara Shah and Manisha Reddy, who assisted me with editing, cite-checking, and researching for this essay. In addition, I would like to thank the *Brooklyn Law Review* editors and staff for their diligence and advice throughout the editing process to make this essay the best it can be. Finally, my heartfelt thanks for the support and encouragement of my three sons, Roshan, Finn, and Leo as well as the constant support and encouragement of my wife Noreen, without which I would not be able to complete this work.

¹ U.S. CONST. amend. I; *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460–61 (1958) (“Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly . . . Of course, it is immaterial whether the beliefs sought to be advanced by association pertain to political, economic, religious or cultural matters, and state action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny.”); Anita L. Allen, *Associational Privacy and the First Amendment: NAACP v. Alabama, Privacy and Data Protection*, ALA. C. R. & C. L. REV. 1, 7 (2011) (“When Americans voluntarily join a private peaceful political, religious, or social association, even an unpopular, controversial one, they are entitled to as much confidentiality as to their names and addresses as the association chooses to confer. The Court ruled that the Due Process Clause of the Fourteenth Amendment confers to each individual the rights of free speech and free association. These are rights protected from federal violation by the First Amendment and from state violation by the First and Fourteenth Amendments.”) (footnote omitted); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 786 (2008) (“[T]he Supreme Court recognized that a government-mandated disclosure of group membership could be an unconstitutional infringement on the right of association.”); Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1386 (2012) (stating “the Court held that the State of Alabama could not compel the NAACP to disclose its membership lists” to the state).

intimidation.² This freedom was promulgated from the freedom of speech and the freedom of assembly under the First Amendment.³ Specifically, the Court has held that ideas expressed through free speech are amplified when brought forth by a group through free assembly that share such ideas.⁴ Further, the U.S. Supreme Court has held that a person has the freedom to be anonymous under the First Amendment;⁵ that is, a person can express creative, political, or commercial speech anonymously.⁶ The reasons for remaining anonymous include economic or political motives, including fear of retaliation from both the government and private entities, such as employers, rival political parties, and more.⁷ Consequently, both the freedom of association and the freedom to be anonymous are touchstones for the foundation of U.S. democracy, which includes the ability to engage in political discourse.⁸

With the advent of the internet and social media, people are organizing themselves into social media groups that share similar political ideas in order to amplify their political speech.⁹ Due to the

² *NAACP*, 357 U.S. at 462 (“Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs”); Strandburg, *supra* note 1, at 787; Swire, *supra* note 1, at 1386.

³ *NAACP*, 357 U.S. at 460–61; *see* Allen, *supra* note 1, at 7; Strandburg, *supra* note 1, at 786–87; Swire, *supra* note 1, at 1386.

⁴ *Boy Scouts of Am. v. Dale*, 530 U.S. 640, 647 (2000) (“[W]e observed that ‘implicit in the right to engage in activities protected by the First Amendment’ is ‘a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends.’” (quoting *Roberts v. United States Jaycees*, 468, U.S. 609, 622 (1984))).

⁵ *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995) (“It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.”); Jason A. Martin and Anthony L. Fargo, *Anonymity as a Legal Right: Where and Why It Matters*, 16 N.C. J. L. & TECH. 311, 330 (2015); A. Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95, 149 (2017) (“[T]he Supreme Court made it clear that there is a sweeping constitutional right to anonymous religious and political speech.”).

⁶ *Watchtower Bible & Tract Soc’y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 166 (2002) (“[R]equiring a permit [not to be anonymous] as a prior condition on the exercise of the right to speak imposes an objective burden on some speech of citizens holding religious or patriotic views.”).

⁷ *See McIntyre*, 514 U.S. at 357; Martin & Fargo, *supra* note 5, at 372; Froomkin, *supra* note 5, at 149.

⁸ *McIntyre*, 514 U.S. at 357; *NAACP*, 357 U.S. at 460–61; Allen, *supra* note 1, at 7; Froomkin, *supra* note 5, 149; Martin & Fargo, *supra* note 5, at 330, 372; Strandburg, *supra* note 1, at 786; Swire, *supra* note 1, at 1386.

⁹ Swire, *supra* note 1, at 1373 (“At Internet conferences that I have attended in the past few years, there have often been panels highlighting how social networks mobilize political change. Speakers on these panels often discussed the 2011 ‘Arab Spring,’ including the ‘Facebook Revolution’ in Egypt that resulted in the overthrow of President Mubarak. They also praised the 2008 Obama campaign, whose outreach and mobilization was led by a co-founder of Facebook. In these panels, a key feature of social networks was their ability to foster political association at the grassroots level—sharing information among activists empowered them.” (footnotes omitted)); Strandburg, *supra* note 1, at 745 (“Digital

nature of social media, many people can be subjected to harassment for their opinions and therefore feel compelled to express creative, commercial, or political ideas anonymously, enabling them to speak honestly and passionately without fear from economic or political reprisal.¹⁰ Thus, any government intrusion upon the freedom of association and the freedom to be anonymous must be viewed with a most critical lens so it does not inhibit people from organizing into social media groups or hiding their identity, which could ultimately chill their political speech on social media.¹¹

The need to express and protect one's opinions electronically—whether anonymously or not—has recently become a contentious political and legal issue in a surprising setting. Since the inauguration of the Trump administration, the U.S. government has made border security a priority.¹² Border security

technology has transformed the ways in which civic and political associations are formed and operate. Nearly every organization now uses email, websites, and cellular phones as primary means of communications with members. Meanwhile, more and more political and civic 'work' in society is performed not by traditionally organized, relatively long-lived, face-to-face associations with well-defined members, leaders, policies, and goals, but by decentralized, often transient, networks of individuals associating only or primarily electronically and with policies and goals defined synergistically with the formation of the emergent association itself." (footnote omitted).

¹⁰ Bethany C. Stein, Comment, *A Bland Interpretation: Why a Facebook "Like" Should Be Protected First Amendment Speech*, 44 SETON HALL L. REV. 1255, 1257 (2014) ("[D]uring a sheriff election, employees of the sheriff's department 'liked' one of the candidate's Facebook page. That candidate lost the election, and when the new sheriff took office he fired the employees who had 'liked' his opponent's Facebook page. The District Court held that 'liking' a Facebook page is not speech that warrants constitutional protection. On appeal, however, the United States Court of Appeals for the Fourth Circuit found that 'liking' a political candidate's Facebook page is speech deserving of First Amendment protection." (footnotes omitted)); Amna Toor, Note, *"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, 290-91 (2018) ("Amid the tense political environment, reports have made their way into the public eye revealing that the Department of Homeland Security ('DHS'), the Federal Bureau of Investigation ('FBI'), and local law enforcement have been conducting surveillance across social media platforms to gather information on #BlackLivesMatter protests and individual activists, and tracking the BLM Movement since 2014... Justice Brennan recognized the importance of preserving the right to freely engage in discussion without fear of censorship [so as to prevent government resentment, hate and instability]." (footnotes omitted)); Maeve Duggan, *Online Harassment 2017* PEW RES. CTR. (July 11, 2017), <http://www.pewinternet.org/2017/07/11/online-harassment-2017/> [<https://perma.cc/8U3F-Q3PZ>].

¹¹ See Swire, *supra* note 1, at 1373; Strandburg, *supra* note 1, at 745; Stein, *supra* note 10, at 1257; Toor, *supra* note 10, at 290–91.

¹² S.M., *Donald Trump's Travel Ban Heads Back to the Supreme Court*, ECONOMIST (Jan. 23, 2018), <https://www.economist.com/blogs/democracyinamerica/2018/01/travelling-ban> [<https://perma.cc/7P3E-QS3D>]; *President Donald J. Trump Wants to Fully Secure Our Border and Reform Our Immigration System to Put America First*, WHITE HOUSE (May 16, 2019), <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-wants-to-fully-secure-our-border-and-reform-our-immigration-system-to-put-america-first/> [<https://perma.cc/DLX9-AP7B>]; Miriam Jordan, *Family Separation May Have Hit Thousands More Migrant Children Than Reported*, N. Y. TIMES (Jan. 17, 2019), <https://www.nytimes.com/2019/01/17/us/family-separation->

has different connotations in this administration; the prevalent policy seeks to prevent illegal immigrants, who are searching for a better way of life, from entering the country. Alternatively, a less publicized, but as important policy for border security, includes blocking terrorists from entering the country.¹³ A terrorist can be defined as a person having an ideology that includes committing violence against a nation or its civilians for a political cause.¹⁴ The Department of Homeland Security (DHS) has instituted rules that allow Customs and Border Patrol (CBP) officials to search the mobile device data of a person entering the country, including his or her social media content, which could potentially provide insight on whether the person has a terrorist ideology.¹⁵

DHS justifies these rules by invoking the border search exception doctrine to the Fourth Amendment. The border search exception doctrine states that a government official or law enforcement officer can conduct a search, without a warrant, of a person and their belongings when entering the United States at the border.¹⁶ The border search exception doctrine views the border or point of entry (i.e., airport, ship dock, etc.) to a country as a vulnerable place for both the sovereignty of the nation and the privacy interest of a person.¹⁷ The underlying rationale of the

trump-administration-migrants.html [https://perma.cc/56AS-QG39] (“The family separations [policy was] a key part of the Trump administration’s effort to deter migrant families from trying to enter the country at the Southwest border.”).

¹³ Lawrence Hurley, *Supreme Court to Decide Legality of Trump Travel Ban*, REUTERS (Jan. 19, 2018, 2:12 PM), <https://www.reuters.com/article/us-usa-court-immigration/supreme-court-to-decide-legality-of-trump-travel-ban-idUSKBN1F82EY> [https://perma.cc/V4CM-DAM9] (stating that the travel was one way the U.S. government hoped to secure the border from terrorists masquerading as refugees to do harm against the United States).

¹⁴ See Roberto Iraola, *Terrorism, the Border, and the Fourth Amendment*, 2003 FED. CTS. L. REV. 1, 20 (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”); *What We Investigate*, FBI, <https://www.fbi.gov/investigate/terrorism> [https://perma.cc/LC39-MMYQ]; Das, *infra* note 20, at 210.

¹⁵ *Inspection of Electronic Devices*, U.S. CUSTOMS & BORDER PROT., <https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf> [https://perma.cc/4D4P-3TTZ]. See Amended Complaint, *infra* note 20, at 28 and 34.

¹⁶ *United States v. Ramsey*, 431 U.S. 606, 619 (1977) (“Boarder searches then, from before the adoption of the Fourth Amendment, have been considered to be ‘reasonable’ by the single fact that the person or item in question had entered into our country from the outside.”); see Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 319 (2015) (“Under the narrow approach, the border search exception exists to allow the government to keep out items that should be outside the United States The underlying right is to control what enters . . . the country.”).

¹⁷ See *Carroll v. United States*, 267 U.S. 132, 153–54 (1925); see also Thomas Mann Miller, *Digital Border Searches After Riley v. California*, 90 WASH. L. REV. 1943, 1996 (2015) (stating that an individual’s privacy interest in their digital data content needs to be balanced with the traditional government interest of preventing people without a legal right to enter the United States from crossing the border and preventing contraband from entering the country); see also Kerr, *supra* note 16, at 294–95 (“The Supreme Court has held that a border search exception to the Fourth Amendment

border search exception is that it is reasonable to search a person and the person's belongings, without a warrant, for the purposes of determining whether the person has a right to enter the country or whether the person is carrying any contraband.¹⁸ No further search is within the scope of the border search exception because not only is the country vulnerable from people attempting to illegally enter the country or carry contraband, but also an individual's privacy interests and constitutional rights are assailable as they may be violated for any number of significant or fickle reasons by border security officials.¹⁹ With these rules, this essay argues that DHS callously intrudes upon the constitutionally protected freedom of association and freedom of anonymity by invoking the border search exception doctrine to search a U.S. citizen's social media accessible through their mobile phone without a warrant when the citizen reenters the United States, thereby chilling the political speech provided by the freedoms of association and anonymity.²⁰

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." (footnotes omitted).

¹⁸ See *Carroll*, 267 U.S. at 153–54; see also Kerr, *supra* note 16, at 294–95.

¹⁹ *United States v. Montoya de Hernandez*, 473 U.S. 531, 552 (1985) (Brennan, J. dissenting) (“[The Fourth Amendment] is, or should be, an important working part of our machinery of government, operating as a matter of course to check the ‘well-intentioned but mistakenly overzealous executive officers’ who are a part of any system of law enforcement” (citing *United States v. United States Dist. Court*, 407 U.S., 297, 315 (1972))).

²⁰ Amended Complaint at 2–3, *Alasaad v. Duke*, No. 1:17-CV-11730-DJC (D. Mass. Sept. 13, 2017), ECF No. 7 (“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.”); Emanuella Grinberg & Jay Croft, *American NASA Scientist Says His Work Phone Was Seized at Airport*, CNN (Feb. 15, 2017, 5:57 PM ET), <http://www.cnn.com/2017/02/13/us/citizen-nasa-engineer-detained-at-border-rnd/index.html> [<https://perma.cc/56RU-HVB4>] (“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.”); *Inspection of Electronic Devices*, *supra* note 15 (“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.”); see Atanu Das, *Crossing the Line*

DHS rules unconstitutionally expand the border search exception doctrine from more than simply ascertaining whether a person can legally enter the United States and whether the person carries contraband, to include a search of their social media content to determine their personal ideology.²¹ This allows DHS personnel to determine whether the person is a terrorist in the name of national security.²² Further, DHS personnel can justify the search of social media content by interpreting language of case law pertaining to border searches broadly with respect to the border search exception doctrine²³ to give CBP officials a wide scope to conduct a warrantless border search of a person and their belongings.²⁴ Once this unbridled authority is more well-known, it has the potential to chill social media political speech made by those most likely targeted as terrorists by CBP officials. DHS, however, have wrongly broadened the scope of the border search exception doctrine.²⁵

Some courts and scholars have been reluctant to exercise any limit to warrantless border searches of data accessible from mobile devices based on the border search exception doctrine under the Fourth Amendment.²⁶ Rather, as this essay argues, framing warrantless border searches of mobile device data as a

Department of Homeland Security Unconstitutional Border Search of Mobile Device Data, 22 U. PA. J. L. & SOC. CHANGE 205, 211 (2019); *see also* U.S. CONST. amend IV.

²¹ Amended Complaint, *supra* note 20, at 28, 34. *See* Iraola, *supra* note 14, at 6–9; *Inspection of Electronic Devices*, *supra* note 15.

²² *See* Iraola, *supra* note 14; *see also* *Inspection of Electronic Devices*, *supra* note 15.

²³ *See* WAYNE R. LAFAYE, 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” (quoting *United States v. Odland*, 502 F.2d 148, 151 (7th Cir. 1974))); *see* *Inspection of Electronic Devices*, *supra* note 15.

²⁴ *United States v. Cotterman*, 709 F.3d 952, 970 (9th Cir. 2013) (en banc) (holding that digital data content on Cotterman’s computer can be lawfully searched without a warrant based on reasonable suspicion); *United States v. Ickes*, 393 F.3d 501, 505 (4th Cir. 2005) (holding that the digital data content on Ickes’s computer can be lawfully searched without a warrant based on reasonable suspicion); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 570–71 (D. Md. 2014) (holding that the digital data content on Saboonchi’s computer can be lawfully searched without a warrant based on reasonable suspicion); *see also* LAFAYE, *supra* note 23, § 10.5(a).

²⁵ *See* *United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977) (finding that some border searches are “particularly offensive” such that there are limits to the scope of border search exception doctrine); *Katz v. United States*, 389 U.S. 347, 361 (1967); *Riley v. California*, 134 S. Ct. 2473, 2495 (2014) (holding that search of data accessible from a mobile device requires a warrant even in situations the mobile device was seized under an exception to the warrant requirement, namely the search incident to arrest exception in this case); Das, *supra* note 20, at 207.

²⁶ *Ramsey*, 431 U.S. at n.13; 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) (“[T]his 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.”); Miller, *supra* note 17, at 1996.

government intrusion upon the freedoms of association and anonymity can be an effective way to constitutionally shield social media content from the CBP officials' prying eyes.²⁷

By discussing the principles of U.S. Supreme Court jurisprudence regarding the freedom of association and the freedom to be anonymous, this essay argues that due to social media groups having constitutional protection under the freedom of association and the freedom of anonymity, warrantless border searches of social media accounts do not meet strict scrutiny. Indeed, these warrantless border searches of electronic data are not narrowly tailored to protect the compelling government interest of national security, thereby unconstitutionally chilling political speech on social media.²⁸

This essay proceeds in the following six parts. Part I outlines a real-life example of the DHS and CBP officials applying the border search exception doctrine to search the contents of a U.S. citizen's mobile phone data. Part II discusses significant Fourth Amendment case law and the border search exception doctrine jurisprudence. Part III and Part IV describe the case law for the freedom of association and the freedom to be anonymous, respectively. Part V applies the freedom of association and freedom to be anonymous to social media. Lastly, Part VI synthesizes these ideas to demonstrate that warrantless border searches of social media infringes upon the freedoms of association and anonymity by chilling political speech.

I. A WARRANTLESS SEARCH OF A U.S. CITIZEN'S MOBILE DEVICE DATA BY AIRPORT BORDER SECURITY

Early in 2017, a thirty-five-year-old U.S.-born citizen Sidd Bikkannavar was stopped by CBP officials at Houston's George Bush Intercontinental Airport while returning to his home in the U.S. from abroad.²⁹ As he was proceeding through immigration review, CBP officials demanded to search the data accessible from his mobile phone.³⁰ His first reaction was to refuse because he was a scientist for the National Aeronautics and Space Administration's (NASA) Jet Propulsion Laboratory in Pasadena,

²⁷ *Riley*, 134 S. Ct. at 2495; *NAACP v. Alabama*, 357 U.S. 449, 460-61 (1958); *McIntyre*, 514 U.S. at 347; *Strandburg*, *supra* note 1, at 748; *Swire*, *supra* note 1, at 1395-96.

²⁸ *NAACP*, 357 U.S. at 460-61; *McIntyre*, 514 U.S. at 347; *Strandburg*, *supra* note 1, at 748; *Swire*, *supra* note 1, at 1374.

²⁹ *Grinberg and Croft*, *supra* note 20. *Das*, *supra* note 20, at 211.

³⁰ Kaveh Waddell, *A NASA Engineer Was Required to Unlock His Phone at the Border* (2017), <https://www.theatlantic.com/technology/archive/2017/02/anasaengineerisrequiredtounlockhisphoneattheborder/516489/> [<https://perma.cc/29VQ-KH43>]; *Das*, *supra* note 20, at 211.

California,³¹ and confidential information was accessible from his mobile phone.³² However, CBP officials gave him an ultimatum to either comply with their demands or have his mobile phone seized until he consented to the search, resulting in Bikkannavar relenting and consenting to the search.³³

After this ordeal, Bikkannavar revealed that CBP officials gave him a document titled “Inspection of Electronic Devices” providing justification that the CBP had the right to search the data accessible from his mobile phone.³⁴ Further, the document stated that a search of this data was mandatory and failure to allow the CBP to do so can result in seizure of the mobile phone.³⁵ The document revealed that a purpose of the warrantless border search of data accessible from a mobile phone was to identify terrorists or to deter terrorist from entering the United States.³⁶

Bikkannavar’s shock was compounded by the fact he had gone through two background checks by the government to determine whether he was a national security risk.³⁷ First, he had gone through a thorough background check as a government employee so that he could access confidential information.³⁸ Second, he applied and was approved for the CPB Protection Global Entry program that expedites his entry in the U.S.³⁹ Neither previous vetting process mattered to CBP officials, as they brow-beat him to consent to a warrantless search of the data accessible from his mobile phone.⁴⁰

Bikkannavar suspected that CBP officials searched his social media as part of their search of his mobile phone. In the fall of 2017, the American Civil Liberties Union (ACLU) sued the DHS on behalf of Bikkannavar and several co-plaintiffs in the United States District Court for the District of Massachusetts to find that the a warrantless border search of mobile device data is unconstitutional in view of both the First Amendment and the Fourth Amendment.⁴¹ Neither the plaintiffs nor the ACLU claimed that the warrantless border search of mobile device data included a search of social media as an unconstitutional government intrusion of the freedom of association and the freedom to be

³¹ Waddell, *supra* note at 30. Das, *supra* note 20, at 211.

³² Waddell, *supra* note at 30. Das, *supra* note 20, at 211.

³³ Grinberg and Croft, *supra* note 20. Das, *supra* note 20, at 211

³⁴ Waddell, *supra* note 30. See Amended Complaint, *supra* note 20, at 23. Das, *supra* note 20, at 212.

³⁵ Waddell, *supra* note 30. Das, *supra* note 20, at 212.

³⁶ *Inspection of Electronic Devices*, *supra* note 15. Das, *supra* note 20, at 212.

³⁷ Waddell, *supra* note 30; Das, *supra* note 20, at 212.

³⁸ Waddell, *supra* note 30; Das, *supra* note 20, at 212.

³⁹ Waddell, *supra* note 30. Das, *supra* note 20, at 212.

⁴⁰ Amended Complaint, *supra* note 20, at 23; Das, *supra* note 20, at 212.

⁴¹ Amended Complaint, *supra* note 20, at 39–40. Das, *supra* note 20, at 212.

anonymous.⁴² Instead, the First Amendment concerns of the plaintiffs were an infringement of freedom of association generally in that there would be a chilling of their friendships and acquaintances due to warrantless border searches of their mobile device data. An amicus brief was filed that also advocated that the warrantless border search of mobile device data infringed upon the freedom of association generally as well as chilling of the freedom of the press.⁴³ The plaintiffs' complaint and the amicus brief did not discuss in any detail that the access to social media accounts through the searched mobile devices infringed on the freedom of association or freedom to be anonymous resulting in a chilling of political speech on social media.⁴⁴ If the plaintiffs did make such a claim, the court would likely hold that it does infringe upon these First Amendment rights.⁴⁵ If the court were to reach such a decision, Bikkannavar or anyone aware of such warrantless border searches of mobile device data would be chilled to express their political or religious beliefs on social media for fear of political retribution from the government.

II. THE FOURTH AMENDMENT AND THE BORDER SEARCH EXCEPTION DOCTRINE JURISPRUDENCE

Prior to understanding the effect of warrantless border searches of mobile device data on the freedom of association and freedom to be anonymous on social media, it is imperative to understand the underpinning of privacy interests of the Fourth Amendment and the border search exception. The Fourth Amendment protects people from unreasonable search and seizures from government law enforcement officers that is guided by the legal principle of a person having a reasonable expectation of privacy.

The border search exception doctrine balances the sovereign's interest to protect the nation from unlawful entry of people and contraband with a person's reasonable expectation of privacy from searches of their person and belongings.⁴⁶ To that extent, the border search exception doctrine applies to both United

⁴² *See id.*

⁴³ Brief of the Knight First Amendment Institute at Columbia University and the Reporters Committee for Freedom of Press as *Amici Curiae* Supporting Plaintiffs at 4-6, *Alasaad v. Duke*, No. 1:17-CV-11730 (D. Mass. Feb. 2, 2018), ECF No. 26.

⁴⁴ *See id.*; *see also* Amended Complaint, *supra* note 20. At this time, the District Court of Massachusetts ruled to deny the motion to dismiss the complaint filed by DHS. Memorandum and Order, *Alasaad v. Duke*, No. 1:17-CV-11730-DJC (D. Mass. May 9, 2018), ECF No. 34.

⁴⁵ *See* *Riley v. California*, 134 S. Ct. 2473, 2495 (2014); *NAACP v. Alabama*, 357 U.S. 449, 460-61 (1958); *McIntyre v. Ohio Elections Com'n*, 514 U.S. 334, 347 (1995); *Strandburg*, *supra* note 1, at 748; *Swire*, *supra* note 1.

⁴⁶ *See* *Katz v. United States*, 389 U.S. 347, 361 (1967); *Carroll v. United States*, 267 U.S. 132, 154 (1925); *Kerr*, *supra* note 16, at 319; *Das*, *supra* note 20, at 212.

States citizens and non-citizens alike. There is some confusion, however, among courts and scholars on whether certain constitutional rights apply to non-citizens. Courts and scholars have come to some consensus that non-citizens may have some constitutional rights if they have some foundational connection to the United States such as residency or a loved one who is a resident or citizen. In contrast, a foreign national who hold a United States visa while visiting the country may have fewer constitutional rights. This essay discusses the effect of the border search exception doctrine on U.S. citizens to simplify the legal analysis.

A. *Fourth Amendment Jurisprudence*

A cornerstone Supreme Court case in the twentieth century regarding the Fourth Amendment is *Olmstead v. United States*.⁴⁷ Although the court's holding was overruled decades later, it is a historical, touchstone case to understand modern Fourth Amendment jurisprudence.⁴⁸ Former President and Chief Justice William Howard Taft authored *Olmstead*, and in this case, the Court had to decide whether a warrantless wiretapping of Roy Olmstead violated the Fourth Amendment.⁴⁹ Law enforcement officers warrantlessly wiretapped Olmstead's office telephones as well as warrantlessly wiretapped his home telephone from the street.⁵⁰ Law enforcement officers did not trespass either Olmstead's office or residence to warrantlessly wiretap the telephones.⁵¹ Consequently, the information collected by law enforcement officers was used to convict Olmstead and his colleagues.⁵²

Chief Justice Taft's analysis from previous Fourth Amendment cases included a trespass doctrine connected to the Fourth Amendment, which protects "material things—the person, the house, his papers, or his effects" because its text states "the warrant . . . must specify the place to be searched and the person or things to be seized."⁵³ Further, Chief Justice Taft stated that although the technology of the telephone extended communications such that two people can talk to each over a great distance,⁵⁴ the Fourth Amendment rights cannot be expanded to protect telephone communications.⁵⁵ In addition, Chief Justice Taft construed that

⁴⁷ See *Olmstead v. U.S.*, 277 U.S. 438, 468 (1928); Das, *supra* note 20, at 213.

⁴⁸ See *Katz*, 389 U.S. at 353; Das, *supra* note 20, at 213.

⁴⁹ *Olmstead*, 277 U.S. at 456–57; Das, *supra* note 20, at 213.

⁵⁰ *Olmstead*, 277 U.S. at 457; Das, *supra* note 20, at 213.

⁵¹ *Olmstead*, 277 U.S. at 457; Das, *supra* note 20, at 213.

⁵² See *Olmstead*, 277 U.S. at 455–56. Das, *supra* note 20, at 213.

⁵³ *Olmstead*, 277 U.S. at 464. U.S. Const. amend. IV. Das, *supra* note 20, at 213.

⁵⁴ *Olmstead*, 277 U.S. at 465; Das, *supra* note 20, at 213.

⁵⁵ *Olmstead*, 277 U.S. at 465; Das, *supra* note 20, at 213.

“intervening wires” of telephone technology are not part of *Olmstead*’s home or office, “any more than are the highways along which they are stretched.”⁵⁶ Therefore, the Court found that “the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment,” which comported with the established trespass doctrine.⁵⁷

Olmstead established the legal foundation that the Fourth Amendment constitutionally protected a person’s place and possessions, but not his intangible voice conversations over the telephone.⁵⁸ *Olmstead*’s narrow holding surprised modern day jurists, which argue that the Fourth Amendment provides broader privacy protections.⁵⁹

Expectedly, the Supreme Court broadened the narrow *Olmstead* holding in subsequent cases and,⁶⁰ almost forty years after *Olmstead*, the Court cured its deficiencies in *Katz v. United States*.⁶¹ Charles Katz was found guilty of violating gaming laws when he gathered betting information over a telephone located in a phone booth in Los Angeles.⁶² FBI agents warrantlessly wiretapped the phone booth to record Katz’s various telephone conversations and⁶³ these recordings were used to convict him.⁶⁴

Justice Potter Stewart, in his majority opinion, found that “the underpinnings of *Olmstead* and *Goldman* have been so eroded . . . [in which] . . . the ‘trespass’ doctrine there enunciated can no longer be regarded as controlling.”⁶⁵ He found that the recordings “violated the privacy upon which [Katz] justifiably relied while using the telephone booth and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment.”⁶⁶ Further, Justice Stewart found that “[t]he fact that the electronic device employed to

⁵⁶ *Olmstead*, 277 U.S. at 465; Das, *supra* note 20, at 213.

⁵⁷ *Olmstead*, 277 U.S. at 466; Das, *supra* note 20, at 213.

⁵⁸ *Olmstead*, 277 U.S. at 466; Das, *supra* note 20, at 213.

⁵⁹ *Olmstead*, 277 U.S. at 361; *Katz*, 389 U.S. at 370 (*Katz* sets the stage for modern Fourth Amendment jurisprudence finding that “[t]o support its new interpretation of the Fourth Amendment, which in effect amounts to a rewriting of the language of the Court’s opinion concludes that ‘the underpinnings of *Olmstead* and *Goldman* have been eroded by our subsequent decisions.’”); see LAFAVE, *supra* note 23, at § 2.1(d) n.127 (citing JM Junker, *The Structure of the Fourth Amendment Scope of the Protection*, 79 J. CRIM. L. & C. 1105, 1125-26 (1989)) (stating “What is remarkable, however, is how little has changed by *Katz*’s abandonment of the ‘trespass’ standard of *Olmstead v. United States*.”); Das, *supra* note 20, at 214.

⁶⁰ *Katz*, 389 U.S. at 353. See LAFAVE, *supra* note 23 at § 2.1(b) (stating that subsequent Supreme Court cases since *Olmstead* eroded its holding thereby expanding Fourth Amendment protections); Das, *supra* note 20, at 214.

⁶¹ *Katz*, 389 U.S. at 370 (Black, J., dissenting). See LAFAVE, *supra* note 23 at § 2.1(d) at n.127; Das, *supra* note 20, at 214.

⁶² *Katz*, 389 U.S. at 348; Das, *supra* note 20, at 214.

⁶³ *Katz*, 389 U.S. at 348; Das, *supra* note 20, at 214.

⁶⁴ *Katz*, 389 U.S. at 348-49; Das, *supra* note 20, at 214.

⁶⁵ *Katz*, 389 U.S. at 353; LAFAVE, *supra* note 23 at § 2.1(b); Das, *supra* note 20, at 214.

⁶⁶ *Katz*, 389 U.S. at 353; Das, *supra* note 20, at 214.

achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance,” thereby destroying the trespass doctrine that the Fourth Amendment only “constitutionally protected places.”⁶⁷ Finally, Justice Stewart stated that Fourth Amendment

considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored “the procedure of antecedent justification that is central to the Fourth Amendment,” a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case.⁶⁸

Katz is considered the foundation modern Fourth Amendment jurisprudence that provides privacy protections to a person from the government.⁶⁹ However, the rule from *Katz* to determine Fourth Amendment protections does not come from Justice Stewart’s majority opinion but from Justice John Marshall Harlan’s concurring opinion.⁷⁰ Justice Harlan concurrence stated that “[m]y understanding of the rule . . . is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”⁷¹ Justice Harlan concluded:

[t]hus a man’s home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the “plain view” of outsiders are not “protected” because no intention to keep them to himself has been exhibited.⁷² On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.⁷³

Thus, *Katz* is the basis of modern Fourth Amendment jurisprudence.⁷⁴ It provides that a person has a privacy protections

⁶⁷ *Katz*, 389 U.S. at 353; see LAFAVE, *supra* note 23 at § 2.1(b); Das, *supra* note 20, at 214.

⁶⁸ *Katz*, 389 U.S. at 359; see LAFAVE, *supra* note 23 at § 2.1(b) (stating “[t]he Court then proceeded to hold that the electronic eavesdropping, although apparently undertaken upon a ‘strong probability’ that *Katz* was using the telephone in violation of federal law, was an unconstitutional search because the agents had not first obtained a warrant”). Das, *supra* note 20, at 214.

⁶⁹ See *Kyllo v. United States*, 533 U.S. 27, 32–33 (2001); Das, *supra* note 20, at 215.

⁷⁰ *Kyllo*, 533 U.S. at 33. LAFAVE, *supra* note 23 at § 2.1(b) (stating “[i]n his concurring opinion in *Katz*, Justice Harlan indicated that he ‘join[ed] the opinion of the Court,’ but then explained what he took that opinion to mean. Because lower courts attempting to interpret and apply *Katz* quickly came to rely upon the Harlan elaboration, as ultimately did a majority of the Supreme Court . . .”); Das, *supra* note 20, at 215.

⁷¹ *Katz*, 389 U.S. at 361; Das, *supra* note 20, at 215.

⁷² *Katz*, 389 U.S. at 361; Das, *supra* note 20, at 215.

⁷³ *Katz*, 389 U.S. at 361; LAFAVE, *supra* note 23 at § 2.1(b); Das, *supra* note 20, at 215.

⁷⁴ See *Kyllo*, 533 U.S. at 32–33; *Riley*, 134 S. Ct. at 2497; Das, *supra* note 20, at 215.

over their possessions, however intangible (e.g. voice conversations, electronic data, etc.) according to the *Katz* reasonable expectation of privacy test.⁷⁵ Based on the *Katz* requirement, if there is a privacy interest in a person's possession, then any reasonable search by the government requires a search warrant based on probable cause.⁷⁶

B. *Border Search Exception Doctrine Jurisprudence*

During the twentieth century, the border search exception doctrine evolved in conjunction with general Fourth Amendment jurisprudence (i.e., *Olmstead* to *Katz*).⁷⁷ The border search exception doctrine was first mentioned in the dicta of *Carroll v. United States*.⁷⁸ In that case, law enforcement officers conducted a vehicle stop on driver George Carroll and searched his vehicle for liquor (which was illegal during Prohibition) in interior Michigan, nowhere near an international border.⁷⁹

As in *Olmstead*, Chief Justice Taft wrote the opinion of the Court.⁸⁰ He opined that although the warrantless search of the automobile took place in interior Michigan, nowhere near an international border, there are several exceptions to the Fourth Amendment requirement of obtaining a warrant.⁸¹ In his dicta, Chief Justice Taft stated such exceptions include not only a vehicle stop, but also a border search.⁸² He went on to state that the Fourth Amendment does not protect a person from any and all warrantless searches but only from *unreasonable* warrantless searches.⁸³ Based on this rationale, Chief Justice Taft surmised that it would be reasonable for a law enforcement officer to stop and search a vehicle without a warrant because a vehicle could flee the jurisdiction prior to obtaining a warrant.⁸⁴ Therefore, he held that it was constitutional for a law enforcement officer to stop and search a suspect's vehicle without a warrant if she or he had probable cause to do so.⁸⁵

⁷⁵ *Katz*, 389 U.S. at 361; *Kyllo*, 533 U.S. at 32–33; *Riley*, 134 S. Ct. at 2497; LAFAVE, *supra* note 23 at § 2.1(b); Das, *supra* note 20, at 215.

⁷⁶ *Katz*, 389 U.S. at 361; Das, *supra* note 20, at 215.

⁷⁷ *Ramsey*, 431 U.S. at n.13; *United States v. Brignoni-Ponce*, 422 U.S. 873, 878 (1975); *Montoya de Hernandez*, 473 U.S. at 539–40; Das, *supra* note 20, at 216.

⁷⁸ *Carroll*, 267 U.S. at 154; LAFAVE, *supra* note 23, at § 10.5(a) (stating that “the United States Supreme Court did not have occasion to pass directly upon the question of whether routine searches of persons or things entering the country are permissible under the Fourth Amendment” until *Carroll v. United States*); Das, *supra* note 20, at 216.

⁷⁹ *Carroll*, 267 U.S. at 134–36; Das, *supra* note 20, at 216

⁸⁰ *Carroll*, 267 U.S. at 134–36; Das, *supra* note 20, at 216

⁸¹ *Carroll*, 267 U.S. at 153–54; Das, *supra* note 20, at 216.

⁸² *Carroll*, 267 U.S. at 153–54; Das, *supra* note 20, at 216–17.

⁸³ *Carroll*, 267 U.S. at 162; Das, *supra* note 20, at 217.

⁸⁴ *Carroll*, 267 U.S. at 153–54; Das, *supra* note 20, at 217.

⁸⁵ *Id.* at 162; LAFAVE, *supra* note 23; Das, *supra* note 20, at 217.

As a result, Chief Justice Taft established the border search exception to the Fourth Amendment as “[t]ravelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.”⁸⁶ Moreover, he stated 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.”⁸⁷ Therefore, the border search exception doctrine was founded upon the rationale that the public interest, which was to determine whether a person can legally enter the United States or whether the person’s possessions included contraband, outweighed the person’s individual privacy rights.⁸⁸ However, any further border search could be unreasonable without a warrant, as indicated in future U.S. Supreme Court jurisprudence.⁸⁹ In *Carroll*, the Court was cognizant, at least implicitly, that the scope of a warrantless border search beyond the limits held in this case may infringe on other freedoms of U.S. citizens as it did with Bikkannavar.

Justice Rehnquist refined the border search exception doctrine in *United States v. Ramsey*.⁹⁰ In this 1977 case, CBP officials justified their warrantless search of envelopes sent in the mail carrying narcotics based on the border search exception doctrine.⁹¹ CBP officials’ suspicions were raised when they found the envelopes were heavier than usual that they originated from Thailand, which was a known source for importing drugs.⁹²

Justice Rehnquist refined the border search exception by stating “[t]hat searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining people and their property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.”⁹³ Citing *Carroll*, he stated that “[i]t would be intolerable and unreasonable if a prohibition agent were

⁸⁶ *Carroll*, 267 U.S. at 154; LAFAVE, *supra* note 23 (stating that border search since the adoption of the Fourth Amendment have been considered “reasonable” by the fact that the person or item in question had entered into the country from outside); Das, *supra* note 20, at 217.

⁸⁷ *Carroll*, 267 U.S. at 149; Das, *supra* note 20, at 217.

⁸⁸ *Id.* at 153–54; Kerr, *supra* note 16, at 319; Das, *supra* note 20, at 217.

⁸⁹ *Ramsey*, 431 U.S. at n.13.

⁹⁰ *Id.* at 617–18; Das, *supra* note 20, at 217.

⁹¹ *Ramsey*, 431 U.S. at 609–10; Das, *supra* note 20, at 217.

⁹² *Ramsey*, 431 U.S. at 609–10; Das, *supra* note 20, at 217.

⁹³ *Ramsey*, 431 U.S. at 616; Das, *supra* note 20, at 217.

authorized to stop every automobile on the chance of finding liquor and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search.”⁹⁴ In addition, Justice Rehnquist reinforced the notion that the border search exception doctrine allows a warrantless search of a person and their belongings to ascertain whether the person can legally enter the United States and whether they carry contraband.⁹⁵ Justice Rehnquist went further to find that there is no requirement for probable cause for a border search.⁹⁶

Buried in a footnote, however, Justice Rehnquist stated that “[w]e do not decide whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it is carried out.”⁹⁷ This footnote acknowledged the limits to warrantless border searches under the border search exception doctrine,⁹⁸ but provided no further guidance. This shows that even Justice Rehnquist believed that some warrantless border searches may be an unconstitutional government intrusion to constitutional protected rights of people entering the country.⁹⁹ The lack of guidance has been seized, however, by the DHS and CBP officials to broaden the purview of warrantless border searches, as they did with *Bikkannavar*,¹⁰⁰ to include searching social media accessible through a citizen’s mobile device, thereby infringing the freedoms of association and anonymity, resulting in the chilling of political speech on social media.

One particularly invasive search and seizure case justified under the border search exception doctrine was in *United States v. Montoya de Hernandez*.¹⁰¹ A cursory review of case may suggest a broadening of scope for the border search exception doctrine,¹⁰² but on deeper review it shows that the conducted search was within conventional scope.¹⁰³ In this 1985 case, CBP officials at Los Angeles International Airport suspected Montoya de Hernandez of smuggling narcotics in her

⁹⁴ *Ramsey*, 431 U.S. at 618; Das, *supra* note 20, at 218.

⁹⁵ *Ramsey*, 431 U.S. at 617–18; Das, *supra* note 20, at 218.

⁹⁶ *Ramsey*, 431 U.S. at 617–18; LAFAVE, *supra* note 23 (stating “[t]he lower courts have consistently held, both before and after *Ramsey*, that routine searches of persons and things may be made upon their entry into the country”); Das, *supra* note 20, at 218.

⁹⁷ *Ramsey*, 431 U.S. at n.13; Das, *supra* note 20, at 218.

⁹⁸ *Ramsey*, 431 U.S. at n.13; Das, *supra* note 20, at 218.

⁹⁹ *Ramsey*, 431 U.S. at n.13. This includes warrantless border searches of people that may not be U.S. Citizens. Das, *supra* note 20, at 218.

¹⁰⁰ See *supra* Part I.

¹⁰¹ *Montoya de Hernandez*, 473 U.S. at 531; Das, *supra* note 20, at 219.

¹⁰² *Montoya de Hernandez*, 473 U.S. at 539; Das, *supra* note 20, at 219.

¹⁰³ *Montoya de Hernandez*, 473 U.S. at 540–41; Das, *supra* note 20, at 219.

alimentary canal.¹⁰⁴ A further search revealed she was wearing a girdle and elastic underpants lined with paper towels that raised further suspicion of the scheme.¹⁰⁵ Consequently, CBP officials held Montoya de Hernandez for sixteen hours to obtain a warrant to conduct a rectal search.¹⁰⁶ The search revealed that Montoya de Hernandez was indeed smuggling drugs in her alimentary canal.¹⁰⁷

Justice Rehnquist found that the border search exception doctrine “[b]alanced against the sovereign’s interests at the border [and] the Fourth Amendment rights of respondent.”¹⁰⁸ Moreover, Justice Rehnquist stated,

respondent was entitled to be free from unreasonable search and seizure.¹⁰⁹ But not only is the expectation of privacy less at the border than in the interior, the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border.¹¹⁰

This led Justice Rehnquist to hold “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.”¹¹¹ Although this case was an example of an invasive warrantless search, it was in the traditional scope of the border search exception doctrine for ascertaining whether a person is carrying contraband into the United States.¹¹²

In contrast, Justice Brennan excoriated Justice Rehnquist in his dissent by analyzing *Montoya de Hernandez* through the lens of *Carroll*, *Ramsey*, and the Fourth Amendment privacy protections described in *Katz*,¹¹³ stating that the search and seizure of Montoya de Hernandez were not that of democratic

¹⁰⁴ *Montoya de Hernandez*, 473 U.S. at 533; LAFAVE, *supra* note 23 at § 10.5(b); Das, *supra* note 20, at 219.

¹⁰⁵ *Montoya de Hernandez*, 473 U.S. at 534; Das, *supra* note 20, at 219.

¹⁰⁶ *Montoya de Hernandez*, 473 U.S. at 535; Das, *supra* note 20, at 219.

¹⁰⁷ *Montoya de Hernandez*, 473 U.S. at 536; LAFAVE, *supra* note 23 at § 10.5(b); Das, *supra* note 20, at 219.

¹⁰⁸ *Montoya de Hernandez*, 473 U.S. at 539; Das, *supra* note 20, at 219.

¹⁰⁹ *Montoya de Hernandez*, 473 U.S. at 539; Das, *supra* note 20, at 219.

¹¹⁰ *Montoya de Hernandez*, 473 U.S. at 539–40 (internal citation omitted); Das, *supra* note 20, at 219.

¹¹¹ *Montoya de Hernandez*, 473 U.S. at 541; LAFAVE, *supra* note 23 at § 10.5(b); Das, *supra* note 20, at 220.

¹¹² *Montoya de Hernandez*, 473 U.S. at 541–42; Das, *supra* note 20, at 220.

¹¹³ *Montoya de Hernandez*, 473 U.S. at 553 (Brennan, J., dissenting); *see also Carroll*, 267 U.S. at 154; *Ramsey*, 431 U.S. at 618 n.13; *Katz*, 389 U.S. at 350; Das, *supra* note 20, at 220.

government.¹¹⁴ Justice Brennan advocated that such an invasive search should only be conducted after obtaining a warrant.¹¹⁵ Such a holding would balance the country's national security concerns with the individual's privacy protections.¹¹⁶ Otherwise, Justice Brennan was afraid that law enforcement officers, motivated by self-interest, may illegally search and seize people at the border.¹¹⁷

Specifically, the border search exception was born from *Carroll*, which allowed a warrantless border search of a person to determine their legal status to enter the United States, and whether their possessions contain any contraband;¹¹⁸ despite this, *Ramsey* found that there may be certain limits to warrantless searches at the border if the search is found to be particularly offensive and *Katz* provides guidance on what are these limits.¹¹⁹

Justice Brennan may have feared that a warrantless border search invades the constitutional rights of U.S. citizens returning to the country, as with *Bikkannavar*.¹²⁰ This buttresses the notion that the warrantless border search of data accessible from a mobile device is a government intrusion upon the rights of freedom of association and the freedom to be anonymous. Such government intrusion is not narrowly tailored to the compelling government interest of national security, the consequence of which chills political speech on social media when CBP officials use the border search exception doctrine to conduct a warrantless border search of mobile device data.¹²¹

Thus, 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 ascertain whether a person can legally enter the United States or whether the person is carrying contraband.¹²² CBP officials, however, have expanded the border search exception doctrine to include warrantless border searches of mobile device data, as in the case of *Bikkannavar*. Such a warrantless border search is an

¹¹⁴ *Montoya de Hernandez*, 473 U.S. 546–50; Das, *supra* note 20, at 220.

¹¹⁵ *Montoya de Hernandez*, 473 U.S. at 552; LAFAVE, *supra* note 23 at § 10.5(b) (stating that the silence of the majority on whether such a search in *Montoya de Hernandez* requires a warrant is particularly significant); Das, *supra* note 20, at 220.

¹¹⁶ *Montoya de Hernandez*, 473 U.S. at 541, 567. This includes a person who may not be a U.S. citizen. Das, *supra* note 20, at 220.

¹¹⁷ *Montoya de Hernandez*, 473 U.S. at 553; Das, *supra* note 20, at 220.

¹¹⁸ *Carroll*, 267 U.S. at 154.

¹¹⁹ *United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977); *Katz*, 389 U.S. at 361.

¹²⁰ *Montoya de Hernandez*, 473 U.S. at 553–54 (Brennan, J., dissenting); *Ramsey*, 431 U.S. at 618 n.13; *see supra* Part I.

¹²¹ *Riley v. California*, 134 S. Ct. 2473, 2495 (2014); *Nat'l Ass'n for Advancement of Colored People v. Alabama*, 357 U.S. 449, 460–61 (1958); *McIntyre v. Ohio Elections Com'n*, 514 U.S. 334, 347 (1995); *Strandburg*, *supra* note 1, at 748; *Swire*, *supra* note 1.

¹²² *See Carroll*, 267 U.S. at 153–54; *see also Kerr*, *supra* note 16, at 294–95.

unconstitutional government intrusion upon the constitutional rights of United States citizens re-entering the country, which, for the reasons stated in the next Parts, includes the freedom of association and the freedom to be anonymous, ultimately stifling political speech on social media.¹²³

III. U.S. SUPREME COURT JURISPRUDENCE ON FREEDOM OF ASSOCIATION

The landmark U.S. Supreme Court case for freedom of association under the First Amendment is *NAACP v. Alabama*.¹²⁴ This 1958 case dealt with a qualifying state statute that required an out-of-state corporation, unless exempt, to file its corporate charter with the Secretary of State and designate a place of business and an agent to serve process.¹²⁵ The Attorney General of Alabama filed suit against the NAACP for failing to comply with the qualifying statute.¹²⁶ The NAACP admitted to non-compliance, believing that non-profit corporations, such as themselves, were exempt from the qualifying statute.¹²⁷ During the course of the suit, the state of Alabama moved for, and the court ordered, the production of membership lists by the NAACP to the state.¹²⁸ The NAACP refused to comply with the production order based on the argument that it violated the First Amendment rights of its members.¹²⁹ The court held the NAACP in contempt and imposed a one hundred thousand dollar fine.¹³⁰ NAACP appealed the decision to the U.S. Supreme Court.¹³¹

Justice Harlan delivered the majority opinion for the Court and found that the production order “trespasse[d] upon fundamental freedoms protected by the Due Process Clause of the Fourteenth,” and the First Amendment.¹³² Further, Justice Harlan stated “[e]ffective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the

¹²³ See *Carroll*, 267 U.S. at 153–54; *Katz*, 389 U.S. at 361; *Ramsey*, 431 U.S. at 618, n.13; *Riley*, 134 S. Ct. at 2495; *NAACP*, 357 U.S. at 460–61; *McIntyre*, 514 U.S. at 347; Strandburg, *supra* note 1, at 748; Swire, *supra* note 1, at 1371.

¹²⁴ *NAACP*, 357 U.S. at 449.

¹²⁵ *Id.* at 451.

¹²⁶ *Id.* at 452.

¹²⁷ *Id.* at 451–53.

¹²⁸ *Id.* at 453.

¹²⁹ *Id.* at 453–54, 460.

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² *Id.* at 460.

freedoms of speech and assembly.”¹³³ Justice Harlan proceeded to state that “[i]t is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the ‘liberty’ assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.”¹³⁴ Moreover, Justice Harlan found that that the freedom of association was indispensable, especially in situations in which the group expresses dissident beliefs.¹³⁵ Also, Justice Harlan opined that revealing the identity of members may risk the members’ well-being through economic, financial, physical, political, and public retribution.¹³⁶ The Court found that the state interest for government intrusion was simply to determine whether the NAACP conducted intrastate business in violation of the qualifying state statute.¹³⁷ Justice Harlan held that such a state interest was not compelling enough to justify infringing on the NAACP members’ freedom of association.¹³⁸ Thus, in *NAACP v. Alabama*, the freedom of association was born as well as the idea that any government intrusion upon this right must be viewed with strict scrutiny.¹³⁹ As described in this essay, the freedom of association can extend to informal social networks as those within social media. Thus, as applied to technology today, an infringement upon the freedom of association by revealing the association of a person to a particular social media group risk economic or political reprisal, the actions of which the freedom of association protects.¹⁴⁰

The freedom of association was further entrenched as a constitutional right in the 1982 U.S. Supreme Court case *Brown v. Socialist Workers ‘74 Campaign Committee*.¹⁴¹ The case dealt with disclosure requirements contained in an Ohio statute that compelled every political party, including a minor political party such as the Socialist Workers Party (SWP), to report the names and addresses of campaign contributors and recipients of campaign disbursements.¹⁴² The SWP filed a class action challenging the constitutionality of the disclosure requirements.¹⁴³ The federal

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ *NAACP*, 357 U.S. at 462.

¹³⁶ *Id.*; see also RONALD D. ROTUNDA & JOHN E. NOWAK, A TREATISE ON CONSTITUTIONAL LAW – SUBSTANCE & PROCEDURE § 20.41(a) (2017).

¹³⁷ *NAACP*, 357 U.S. at 464.

¹³⁸ *Id.* at 464–66.

¹³⁹ *Id.* at 466.

¹⁴⁰ See Stein, *supra* note 10. See Toor, *supra* note 10.

¹⁴¹ *Brown v. Socialist Workers ‘74 Campaign Comm.* (Ohio), 459 U.S. 87, 91–92 (1982).

¹⁴² *Id.* at 88.

¹⁴³ *Id.* at 89.

district court found the disclosure requirements unconstitutional but the decision was appealed to the U.S. Supreme Court.¹⁴⁴

Justice Marshall delivered the majority opinion for the Court¹⁴⁵ and found that “[t]he Constitution protects against the compelled disclosure of political associations and beliefs. Such disclosures ‘can seriously infringe on the privacy association and belief guaranteed by the First Amendment.’”¹⁴⁶ In addition, Justice Marshall stated that the Ohio statute is subject to exacting scrutiny, which requires that the statute must have a “substantial relation between the information sought and [an] overriding and compelling state interest.”¹⁴⁷ Furthermore, the Court found “three government interests sufficient in general to justify requiring disclosure of information concerning campaign contributions and expenditures: enhancement of voters’ knowledge about a candidate’s possible allegiances and interests, deterrence of corruption, and the enforcement of contribution limitations.”¹⁴⁸ These sufficient government interests were found to be requirements for major political parties rather than for minor political parties such as SWP.¹⁴⁹ With the irrelevant government interest, Justice Marshall found that the disclosure requirements were unconstitutional.¹⁵⁰ That is, the Court held that for minor political parties, the freedom of association not only applies to campaign contributors, but also the recipients of the campaign disbursements.¹⁵¹

The Court also found that “[t]he First Amendment prohibit[ed] a state from compelling disclosures by a minor party” if there is a “reasonable probability of threats, harassment, or reprisals.”¹⁵² Thus, since the government intrusion was not substantially related to a compelling government interest, the Court found the Ohio statute unconstitutional.¹⁵³ The Court’s finding of threats, harassments, and reprisals in the context of *Socialist Workers ‘74 Campaign Committee* can be applied to the social media context. Revelation of a person’s association to an

¹⁴⁴ *Id.* at 90.

¹⁴⁵ *Id.* at 88.

¹⁴⁶ *Id.* at 91 (quoting *Buckley v. Valeo*, 424 U.S. 1, 64 (1976)).

¹⁴⁷ *Id.* at 92 (quoting *Gibson v. Florida Legislative Comm.*, 372 U.S. 539, 546 (1963) (internal quotation marks omitted)).

¹⁴⁸ *Id.* (citing *Buckley v. Valeo*, 424 U.S. 1, 60–74 (1976) (footnotes omitted)).

¹⁴⁹ *Id.* at 95

¹⁵⁰ *Id.* at 95–98.

¹⁵¹ *Id.* at 97–98.

¹⁵² *Id.* at 101; *Nat’l Ass’n for Advancement of Colored People v. Alabama*, 357 U.S. 449, 462 (1958); *Strandburg*, *supra* note 1, at 790.

¹⁵³ *Brown*, 459 U.S. at 101–02. Note, that in this case, a less than strict scrutiny is used due to the electoral context of the intruding government regulating statute. *See id.* at 92–95 (1982). However, in other contexts, any government intrusion to the freedom of association is subject to strict scrutiny. *NAACP*, 357 U.S. at 461; *Strandburg*, *supra* note 1; *Swire*, *supra* note 1, at 1387.

unpopular social media group, especially with a political affiliation would subject the person to economic or political retribution. Thus, an infringement of the freedom of association can chill a person from joining such a social media group.

In the 2000 case *Boy Scouts of America v. Dale*, James Dale sued the Boy Scouts of America for revoking his membership based on his homosexuality, asserting that it was in violation of New Jersey's public accommodation law,¹⁵⁴ which stated that "discrimination on the basis of sexual orientation in places of public accommodation" is prohibited.¹⁵⁵ In their reasons for revoking James Dale's membership, the Boy Scouts argued that homosexuality was against their values.¹⁵⁶ According to the Boy Scouts, the case was framed as New Jersey's public accommodation law representing an unconstitutional government intrusion upon the group's freedom of association.¹⁵⁷

Chief Justice Rehnquist delivered the majority opinion of the Court¹⁵⁸ and found that the First Amendment provides the right to associate with others to pursue a common political, social, economic, educational, religious, and cultural views.¹⁵⁹ In addition, Chief Justice Rehnquist stated that that the freedom of association also includes the freedom not to associate.¹⁶⁰ Moreover, Chief Justice Rehnquist opined that the government cannot be one which attempts to regulate the internal affairs of a group by trying to force the group to accept a member they do not desire.¹⁶¹ In this case, Chief Justice Rehnquist found that the compelling state interest was prohibiting discrimination based on sexual orientation.¹⁶² The Court found, however, that determining whether the public accommodation law was narrowly tailored to a compelling state interest was not the proper context for this case.¹⁶³ Further, the Court contemplated whether James Dale could be admitted into the Boy Scouts of America or not.¹⁶⁴ The Court suggested that the proper framework to analyze the public accommodation law was whether the admission of James Dale would be a significant burden on the Boy Scouts of America expression that homosexuality is an immoral way of life.¹⁶⁵ In the

¹⁵⁴ *Boy Scouts of Am. v. Dale*, 530 U.S. 640, 644–45 (2000).

¹⁵⁵ *Id.* (citing N.J. STAT. ANN. §§ 10:5-4–10:5-5 (West Supp. 2000)).

¹⁵⁶ *Id.* at 643, 651.

¹⁵⁷ *Id.* at 659.

¹⁵⁸ *Id.* at 643.

¹⁵⁹ *Id.* at 647 (citing *Roberts v. United States Jaycees*, 468 U.S. 609, 622 (1984)).

¹⁶⁰ *Id.* at 648 (citing *Roberts v. United States Jaycees*, 468 U.S. 609, 623 (1984)).

¹⁶¹ *Id.* (quoting *Roberts v. United States Jaycees*, 468 U.S. 609, 623 (1984)).

¹⁶² *Id.* at 657.

¹⁶³ *Id.* at 659.

¹⁶⁴ *Id.*

¹⁶⁵ *Id.*

framework of this judicial analysis, Chief Justice Rehnquist held that the “First Amendment prohibits the State from imposing” forced admission of a homosexual member into the Boy Scouts of America through its public accommodation law.¹⁶⁶ Thus, in view of U.S. Supreme Court jurisprudence, any government intrusion upon the freedom of association must be narrowly tailored to a compelling government interest, even when the compelling interest is an interest as serious as preventing discrimination.¹⁶⁷

The freedom of association can and should be applied to social media groups because being a member of a social media group can be a form of expression protected by the First Amendment in view of the above Supreme Court jurisprudence. Thus, any government intrusion, such as revealing whether a person is a member of such a social media group, would infringe upon the freedom of association. A warrantless border search of mobile device data is a government intrusion that would infringe upon the freedom of association on social media resulting in suppressing people from associating themselves with any political social media group, formal or informal, for fear of political retribution.

IV. U.S. SUPREME COURT JURISPRUDENCE ON FREEDOM TO BE ANONYMOUS

The landmark case regarding the freedom to be anonymous is *McIntyre v. Ohio Elections Commission*,¹⁶⁸ which concerned “an Ohio statute . . . prohibit[ing] the distribution of anonymous campaign literature.”¹⁶⁹ In 1988, a school district official found out that Margaret McIntyre anonymously distributed pamphlets opposing a local tax levy¹⁷⁰ and filed a complaint against her with the Ohio Elections Commission.¹⁷¹ As a result, the Ohio Elections Commission fined Margaret McIntyre one hundred dollars in accordance with the Ohio statute.¹⁷²

Justice John Paul Stevens delivered the majority opinion of the Court¹⁷³ and held that the First Amendment not only protects the freedom to publish creative literature anonymously,

¹⁶⁶ *Id.*; see also ROTUNDA & NOWAK, *supra* note 136, at § 20.41(d).

¹⁶⁷ *Boy Scouts of Am.*, 530 U.S. at 645, 658–60; Nat’l Ass’n for Advancement of Colored People v. Alabama, 357 U.S. 449, 461 (1958); Strandburg, *supra* note 1; Swire, *supra* note 1, at 1387.

¹⁶⁸ *McIntyre v. Ohio Elections Com’n*, 514 U.S. 334 (1995).

¹⁶⁹ *Id.* at 336.

¹⁷⁰ *Id.* at 337.

¹⁷¹ *Id.* at 338.

¹⁷² *Id.*

¹⁷³ *Id.* at 336.

but also protects the freedom to publish political literature.¹⁷⁴ In addition, Justice Stevens stated that a person expresses political speech anonymously to protect themselves from reprisal and a law that reveals a person's identity destroying their anonymity burdens political speech; such a law that burdens political speech should be subject to at least exacting scrutiny to determine whether the law is narrowly tailored to a state interest.¹⁷⁵ The state of Ohio argued that it had two compelling interests for the statute: (1) "preventing fraudulent or libelous statements"; and (2) "providing the electorate with relevant information" (i.e. informed electorate).¹⁷⁶ Justice Stevens held that "[a]nonymity is a shield from tyranny of the majority"¹⁷⁷ and that "society accords greater weight to the value of free speech than to the dangers of its misuse."¹⁷⁸ Thus, the Court held that the Ohio statute was an unconstitutional government intrusion upon the freedom to be anonymous because it was not narrowly tailored to serve the Ohio's asserted compelling interest.¹⁷⁹ Moreover, the freedom anonymity can extend to the warrantless border search of mobile device data including social media.¹⁸⁰ Government inspection of a person's social media destroys their anonymity and chills subsequent political speech for that person in particular and for the populous as a whole.¹⁸¹

Similarly, in the 2002 case of *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton*, the Court dealt with a religious group seeking an injunction of a village ordinance requiring door-to-door advocates to register with the mayor in order to receive a permit to canvass neighborhoods in the village.¹⁸² The religious group argued that the village ordinance violated their First Amendment rights such as the freedom to exercise religion, freedom of speech, and freedom of press.¹⁸³ The Court granted certiorari to answer the legal question of whether the ordinance violated the First Amendment protection to anonymously provide pamphlets

¹⁷⁴ *Id.* at 342–43.

¹⁷⁵ *Id.* at 347–48.

¹⁷⁶ *Id.* at 348.

¹⁷⁷ *Id.* at 357.

¹⁷⁸ *Id.*

¹⁷⁹ *Id.*

¹⁸⁰ See Duggan, *supra* note 10, which states that fourteen percent of people surveyed in a Pew Research study were harassed on social media due to their political views implying that anonymity in expressing political speech would be valued by a significant portion of American society, especially anonymity from government officials.

¹⁸¹ *Id.* If people know that the government can inspect their social media, through a warrantless border search, thereby destroying their anonymity, they will more likely not express their political views.

¹⁸² *Watchtower Bible and Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 153 (2002).

¹⁸³ *Id.* at 153–54.

and discourse door-to-door.¹⁸⁴ The Court examined the alleged violation of the freedom to be anonymous, mentioning that there was some evidence that the mayor had shown hostility toward the religious group.¹⁸⁵ In conjunction with evidence of the hostility shown from the mayor, other evidence pointed to the fact that the religious group was concerned about political retribution from the mayor if they had to register for a permit and reveal their identity.¹⁸⁶

In delivering the majority opinion for the Court,¹⁸⁷ Justice Stevens debated the level of scrutiny to apply to the village ordinance and ultimately settled on strict scrutiny.¹⁸⁸ The village stated the ordinance addressed several compelling interests, including prevention of fraud, crime, and protection of residents' privacy.¹⁸⁹ Justice Stevens found that the village ordinance covered a wide range of free speech that included political speech, religious speech, and commercial speech.¹⁹⁰ Further, the Justice stated that if prevention of fraud was a compelling interest, then the village ordinance would only cover commercial speech and no other types of speech.¹⁹¹ Indeed, the Court found that it was unlikely that requiring a permit would deter criminals to canvass door-to-door¹⁹² because criminals commit crimes with or without the village ordinance, such as use some other pretext instead of canvassing, to knock on the door of a residence to commit a crime.¹⁹³

Thus, Justice Stevens found that the village ordinance was too broad. Not only did it try to address the criminal and privacy concerns, but it also burdened religious and political speech. With respect to residential privacy, Justice Stevens stated that a resident could simply refuse to engage with a door-to-door canvasser if she or he did not want to listen to the canvasser.¹⁹⁴ Therefore, the Court held that the village ordinance was not narrowly tailored to serve a compelling government interest, and therefore unconstitutionally intruded upon the freedom to be anonymous.¹⁹⁵ Lastly, and most importantly, the Court stated that the freedom to be anonymous is crucial to the country's political discourse and functioning as a democracy, and

¹⁸⁴ *Id.* at 160.

¹⁸⁵ *Id.* at 158.

¹⁸⁶ *Id.*

¹⁸⁷ *Id.* at 153.

¹⁸⁸ *Id.* at 164, 168.

¹⁸⁹ *Id.* at 164–65.

¹⁹⁰ *Id.* at 165.

¹⁹¹ *Id.*

¹⁹² *Id.* at 169.

¹⁹³ *Id.*

¹⁹⁴ *Id.* at 168.

¹⁹⁵ *Id.*

any governmental intrusion upon this freedom must be subject to strict scrutiny.¹⁹⁶

In view of the above Supreme Court jurisprudence, the freedom of anonymity can and should be applied to users of social media. Any government intrusion that reveals the identity of a social media user expressing political speech would infringe upon the freedom of anonymity. A warrantless border search of mobile device data is such a government intrusion because it would infringe upon the freedom to be anonymous on social media, ultimately silencing people from expressing their political beliefs for fear of political or government reprisal.

V. U.S. SUPREME COURT JURISPRUDENCE ON FREEDOM OF ASSOCIATION AND FREEDOM TO BE ANONYMOUS APPLIES TO SOCIAL MEDIA

A. *Freedom of Association Applies to Social Media*

Although the freedom of association applies to groups that have formal relationships between the group governing body and its members, such as social activist groups, political parties, and service groups, the freedom of association can also apply to informal groups as well.¹⁹⁷ A person's informal relationships, such as social and professional circles, are associations that are protected by the freedom of association.¹⁹⁸ Government interference of such personal relationships would chill the populous as each person would be looking over their shoulder to see whether government surveillance would catch them in an intimate, associational relationship, which is antithetical to the ideology of democratic government.¹⁹⁹ For example, organizing a protest for a social cause opposing a government policy by an informal group should be protected from government intrusion under the freedom of association.²⁰⁰

Today, people use social media as a tool to organize into formal and informal groups for a specific common political,

¹⁹⁶ *Id.* at 167–68.

¹⁹⁷ Swire, *supra* note 1, at 1377 (“Social networks serve as platforms for what freedom of association doctrine calls ‘expressive’ associations, such as political groups, religious organizations, and other groups in civil society.”). Further, Swire points out that social media were crucial in the “Arab Spring” political movement in the Middle East and Africa as well as the grassroots movement during President Obama’s campaign. *Id.* at 1379; *see also* Strandburg, *supra* note 1, at 804–05 (stating that expressive association of informal social networks can be protected under the freedom of association).

¹⁹⁸ *See* Swire, *supra* note 1, at 1377; Strandburg, *supra* note 1, at 804–05.

¹⁹⁹ *See* Strandburg, *supra* note 1, at 745; Toor, *supra* note 10, at 323.

²⁰⁰ Swire, *supra* note 1, at 1377, 1379.

economic, social, religious, professional, or creative cause.²⁰¹ In addition, people use social media to express their individual political and social views as part larger collective voice.²⁰² The freedom of association protects all of this speech from government intrusion under the First Amendment.²⁰³

Although people may share even an informal membership in a social media group with friends, a social media platform, and other third parties, these same people would not want to disclose such an informal membership into the social media group to the government.²⁰⁴ Further, disclosure to the government of one's informal membership to a social media group instills a fear of retribution, however slight, by the government.²⁰⁵ Such fear chills the person from organizing herself into certain social media groups and expressing certain political speech on social media.²⁰⁶ This political chilling effect is antithetical to the First Amendment rights of the country's values and also undermines political discourse, which is part of the foundation of the nation's democracy.²⁰⁷

B. *Freedom to Be Anonymous Applies to Social Media*

Sometimes people wish to remain anonymous when using social media.²⁰⁸ In this regard, being anonymous does not necessarily mean people wish to hide their identity from everyone all the time.²⁰⁹ Instead, it may mean hiding their identity from a particular entity, such as hackers, government, employer, or advertisers, for a period of time.²¹⁰ As a recent Pew Research study

²⁰¹ Strandburg, *supra* note 1, at 801; Swire, *supra* note 1, at 1377.

²⁰² Toor, *supra* note 10, at 288–93; Swire, *supra* note 1, at 1377–79.

²⁰³ Strandburg, *supra* note 1, at 801–05; Toor, *supra* note 10, at 293; Swire, *supra* note 1, at 1380, 1396, 1415; NAACP, 357 U.S. at 466.

²⁰⁴ Strandburg, *supra* note 1, at 804–05; Toor, *supra* note 10, at 293; Swire, *supra* note 1, at 1406.

²⁰⁵ Strandburg, *supra* note 1, at 804–05; Toor, *supra* note 10, at 297; Stein, *supra* note 10, at 1275.

²⁰⁶ Strandburg, *supra* note 1, at 805; Stein, *supra* note 10, 1274–75.

²⁰⁷ Toor, *supra* note 10, at 312–13; Stein, *supra* note 10, at 1256.

²⁰⁸ Fernando L. Diaz, *Trolling & the First Amendment: Protecting Internet Speech in the Era of Cyberbullies & Internet Defamation*, U. ILL. J. L. TECH. & POL'Y 135, 147 (2016); Daegon Cho & Soodong Kim, *Empirical Analysis of Online Anonymity and User Behaviors: the Impact of Real Name Policy*, 2012 45th Hawaii International Conference on System Sciences 3041, 3046–47 (comparing the quantity of social media postings before and after the Real Name Verification Law in South Korea was enacted. The study found a significant decrease of social media postings after the law was enacted that eliminated anonymity on the Internet for South Koreans.).

²⁰⁹ Strandburg, *supra* note 1, at 745–46. Although people form online social groups in which members of groups are known to each other, the members of these groups may still want to be anonymous with respect to the government.

²¹⁰ Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PEW RES. CTR. (Sept. 5, 2013), <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/> [https://perma.cc/4SZY-9BJH].

shows, eighty-six percent of adult internet users perform some function to reduce their visibility to some entity.²¹¹ In addition, the Pew Research study shows people try to hide their identity the most from hackers, but only five percent hide their identity from the government.²¹² However, as it becomes more known that the government may surveil online social groups to a certain extent, members of these online social media groups may want to hide their identity from the government.²¹³

Moreover, a recent study of the effect of a South Korean law requiring real name identification online and criminalizing anonymity for its residents shows a substantial effect on behavior.²¹⁴ A significant number of participants in the study were shown to have marked decline in uninhibited behaviors after the law came into effect and were more discreet in their online behavior.²¹⁵ Thus, this indicates that if there was such a U.S. government intrusion upon the freedom to be anonymous by surveilling people's social media, it would suppress their political speech on social media, thereby crumbling the marketplace of political ideas, which is lifeblood to any democracy.²¹⁶

C. *Recent U.S. Supreme Court Cases Regarding the Constitutional Privacy Protections of Mobile Device Data Bolster the Freedom of Association and Freedom to be Anonymous on Social Media*

Although there has been no U.S. Supreme Court case dealing with the freedom of association and the freedom to be anonymous regarding mobile devices and social media accounts, the Court has dealt with the warrantless search of mobile devices in other contexts.²¹⁷

In *Riley v. California*, a 2014 case dealing with the search incident to arrest exception to the warrant requirement under the Fourth Amendment rather than the border search exception doctrine, police officers conducted a vehicle stop on David Leon Riley's vehicle for expired registration tags.²¹⁸ During the vehicle stop, the police officers discovered that Riley was driving with a

²¹¹ *Id.* at 4.

²¹² *Id.* at 5.

²¹³ Cho & Kim, *supra* note 208; Strandburg, *supra* note 1, at 745–46.

²¹⁴ Cho & Kim, *supra* note 208, at 3046–47.

²¹⁵ *Id.*

²¹⁶ *McIntyre*, 514 U.S. at 357; *Watchtower Bible and Tract Society*, 536 U.S. at 165–66; *Froomkin*, *supra* note 5, at 145.

²¹⁷ *Riley*, 134 S. Ct. at 2480–81.

²¹⁸ *Id.* at 2480; Das, *supra* note 20, at 230.

suspended license.²¹⁹ As a matter of routine, Riley's vehicle was impounded;²²⁰ additionally, while conducting an inventory search, police officers found two concealed firearms in the vehicle.²²¹ This led to Riley's arrest for possession of concealed firearms.²²² Incident to arrest, the police seized a mobile phone as well as personal items that revealed Riley was a member of a gang.²²³ The police officers went a step further by searching the contents of the mobile phone discovering images of Riley near a car involved in a shooting a few weeks earlier.²²⁴ As a result, Riley was charged with the shooting.²²⁵ During his legal proceedings, Riley moved to suppress the evidence discovered on his mobile phone by the police officers on the basis that it was a warrantless search out of scope of the search incident to arrest exception.²²⁶

Chief Justice John Roberts, in his majority opinion that stated the scope of a warrantless search incident to arrest is to remove any weapons that pose a threat to law enforcement while apprehending the suspect (be it in an automobile, residence, or in public) and avoid destruction of evidence.²²⁷ Further, he found "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.'"²²⁸ Thus, the Court found that the government intrusion of a warrantless search of mobile device data incident to an arrest is subject to strict scrutiny.²²⁹

In addition, Chief Justice Roberts justified the scope of the search incident to arrest exception by its historical foundation,²³⁰ resulting in a finding that "[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."²³¹ Indeed, law enforcement officers can conduct a warrantless search of the mobile phone incident to arrest to determine whether it is

²¹⁹ *Riley*, 134 S. Ct. at 2480–81; Das, *supra* note 20, at 230.

²²⁰ *Riley*, 134 S. Ct. at 2480–81; Das, *supra* note 20, at 230.

²²¹ *Riley*, 134 S. Ct. at 2480–81; Das, *supra* note 20, at 230.

²²² *Riley*, 134 S. Ct. at 2480–81; Das, *supra* note 20, at 230.

²²³ *Riley*, 134 S. Ct. at 2480–81; Das, *supra* note 20, at 230.

²²⁴ *Riley*, 134 S. Ct. at 2480–81; Das, *supra* note 20, at 230.

²²⁵ *Riley*, 134 S. Ct. at 2481; Das, *supra* note 20, at 230.

²²⁶ *Riley*, 134 S. Ct. at 2481; Das, *supra* note 20, at 230.

²²⁷ *Riley*, 134 S. Ct. at 2482, 2485; Das, *supra* note 20, at 230.

²²⁸ *Riley*, 134 S. Ct. at 2484; Das, *supra* note 20, at 230.

²²⁹ Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1280–81 (June 2007); *Riley*, 134 S. Ct. at 2484.

²³⁰ *Riley*, 134 S. Ct. at 2483–84; Das, *supra* note 20, at 230.

²³¹ *Riley*, 134 S. Ct. at 2485; Das, *supra* note 20, at 230.

disguising any weapons; (e.g., a bomb may be hidden within the mobile phone)²³² however, once it is determined that the mobile phone is not hiding any weapons, any further search of the mobile phone is out of scope of the search incident to arrest exception.²³³ Moreover, Chief Justice Roberts addressed the destruction of evidence aspect of the search incident to arrest by stating “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.”²³⁴

Thus, the purpose of the search incident to arrest exception is to allow a warrantless search to protect law enforcement officers from hidden weapons and to prevent destroying of evidence.²³⁵ The Court held that any further search, including the data accessible by a mobile phone, required a search warrant based on probable cause because a mobile phone is not simply used as telephone but can also be used as a storage device containing details of a person’s life she or he would like to keep private.²³⁶ Such details are ones must be given the strongest of constitutional protection and any government intrusion of which should be subject to strict scrutiny.²³⁷ Although Chief Roberts held that such constitutional protection is shielded by the Fourth Amendment, the holding can be interpreted to bolster the freedom of association and the freedom to be anonymous on social media accessible through a mobile device.²³⁸

This rationale from the ruling in *Riley*, which applies to the search incident to arrest exception to the warrant requirement, can also be applied to any warrantless border search under the border search exception doctrine.²³⁹ That is, after a warrantless border search determines that a person can legally enter the United States and carries no contraband, any further search, including a search of a person’s mobile device data, is warrantless government surveillance of a person’s social media and must be subject to strict scrutiny because it is a

²³² *Riley*, 134 S. Ct. at 2485; Das, *supra* note 20, at 230.

²³³ *Riley*, 134 S. Ct. at 2485; Das, *supra* note 20, at 230.

²³⁴ *Riley*, 134 S. Ct. at 2486; Das, *supra* note 20, at 231.

²³⁵ *Riley*, 134 S. Ct. at 2485–86; Das, *supra* note 20, at 231.

²³⁶ *Riley*, 134 S. Ct. at 2494–95; Das, *supra* note 20, at 231.

²³⁷ *Riley*, 134 S. Ct. at 2494–95.

²³⁸ *Riley*, 134 S. Ct. at 2495; Strandburg, *supra* note 1, at 741; Swire, *supra* note 1, 1374–75.

²³⁹ *Ramsey*, 431 U.S. at 621; *Riley*, 134 S. Ct. at 2494–95; Das, *supra* note 20, at 231.

government intrusion upon the freedom of association and the freedom to be anonymous.²⁴⁰

Likewise, the 2018 case *Carpenter v. United States* dealt with law enforcement officials gathering location information about Carpenter provided by his mobile phone to his cell phone provider in Michigan and Ohio.²⁴¹ Using the location information collected from the cell phone carrier without a warrant, law enforcement officers were able to place Carpenter at several robberies.²⁴² Carpenter filed a motion to suppress the location information as violating his reasonable expectation of privacy under the Fourth Amendment.²⁴³

Chief Justice Roberts wrote the opinion of the Court, holding that although Carpenter provided his location information to the third-party, the cell phone carrier, such location information was so intimate to his constant whereabouts that it was constitutionally protected information and that Carpenter had a reasonable expectation of privacy of his location information under the Fourth Amendment.²⁴⁴ 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.²⁴⁵ Chief Justice Roberts found that because location information of a mobile device is so intimate, it requires the highest level of constitutional protection.²⁴⁶

Applying *Carpenter's* rationale to a warrantless border search of mobile device data, a person's social media is as intimate as a person's location information.²⁴⁷ That is, a person's social media can include her or his political and social views that they would want to constitutionally shield from government surveillance.²⁴⁸ Thus, a person's social media should receive the same level of constitutional protection as the person's location information.²⁴⁹ Such a level of constitutional protection includes protecting a person's social media accessible through a mobile device from government surveillance under the freedom of association and the freedom to be anonymous.

²⁴⁰ *Ramsey*, 431 U.S. at 616; *Riley*, 134 S. Ct. at 2484, 2495; Strandburg, *supra* note 1, at 741; Swire, *supra* note 1, at 1373–74; Fallon, *supra* note 229, at 1280.

²⁴¹ *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018); Das, *supra* note 20, at 231.

²⁴² *Carpenter* 138 S. Ct. at 2206, 2212; Das, *supra* note 20, at 231.

²⁴³ *Carpenter* 138 S. Ct. at 2206, 2212.

²⁴⁴ *Id.* at 2211, 2220; Das, *supra* note 20, at 232.

²⁴⁵ *Carpenter* 138 S. Ct. at 2221; Das, *supra* note 20, at 232.

²⁴⁶ *Id.* at 2217.

²⁴⁷ Toor, *supra* note 10, at 313–14; Stein, *supra* note 10, at 1266.

²⁴⁸ Toor, *supra* note 10, at 311–13; Stein, *supra* note 10, at 1266–68.

²⁴⁹ *Carpenter* 138 S. Ct., at 2222–23; Toor, *supra* note 10, at 301; Stein, *supra* note 10.

VI. WARRANTLESS BORDER SEARCH OF SOCIAL MEDIA IS AN UNCONSTITUTIONAL GOVERNMENT INTRUSION UPON THE FREEDOM OF ASSOCIATION AND TO THE FREEDOM TO BE ANONYMOUS

As mentioned in Part I, CPB officials subjected Bikkannavar to a warrantless border search of his mobile device data. Although the ACLU sued the DHS on Bikkannavar's and the co-plaintiffs' behalf, arguing that such warrantless border searches infringe upon their First Amendment rights generally, it did not specifically state that the warrantless border search of social media accessible through their mobile device infringes their freedoms of association and anonymity, chilling their political speech.²⁵⁰

Courts may not be aware of the extent that searches of mobile technology and government intrusion can infringe on such freedoms. A Pew Research study shows that seventy-seven percent of people in the United States own a smartphone and sixty-nine percent of the people use social media.²⁵¹ Considering the ease in which to access social media using a smartphone, it is likely that almost all of those that use social media access it through their smartphone.²⁵² Any government surveillance of social media is a government intrusion that would affect a significant number of U.S. citizens, some of which would be chilled in expressing any political speech on social media.²⁵³ Further, the DHS policy for a warrantless border search of mobile device data includes a mandate to determine whether a person entering the United States is a terrorist.²⁵⁴ One way in which to determine whether a person entering the United States has a terrorist ideology would be to conduct a warrantless border search of social media accessible through their mobile device.²⁵⁵ Such government surveillance is also a government intrusion upon the freedom to associate into social media groups as well

²⁵⁰ See *supra* Part I.

²⁵¹ JACOB POUSHTER, CALDWELL BISHOP, & HANYU CHWE, PEW RES. CTR. SOCIAL MEDIA USE CONTINUES TO RISE IN DEVELOPING COUNTRIES BUT PLATEAUS ACROSS DEVELOPED ONES 14, 16 (2018), <http://www.pewglobal.org/2018/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones/> [<https://perma.cc/2MRA-5P4H>].

²⁵² Toor, *supra* note 10, at 314; Stein, *supra* note 10, 1255–56; POUSHTER, BISHOP, & CHWE, *supra* note 251.

²⁵³ See generally Toor, *supra* note 10; Stein, *supra* note 10; POUSHTER, BISHOP, & CHWE, *supra* note 241; Allen, *supra* note 1; Strandburg, *supra* note 1. Swire, *supra* note 1; Martin & Fargo, *supra* note 5; Froomkin, *supra* note 5; Fallon, *supra* note 229.

²⁵⁴ *Inspection of Electronic Devices*, *supra* note 15; Amended Complaint, *supra* note 20, at 16–18.

²⁵⁵ *Inspection of Electronic Devices*, *supra* note 15; Motion to Dismiss, *supra* note 44, at 16–18; Iraola, *supra* note 14.

as being anonymous on social media, especially through a person's smartphone, and is subject to strict scrutiny.²⁵⁶

As described in this essay, the strict scrutiny analysis of a government intrusion upon the freedoms of association and anonymity means that it must be narrowly tailored to a compelling government interest.²⁵⁷ The compelling government interest for a warrantless border search is a matter of national security, specifically, preventing terrorists from entering the United States.²⁵⁸ Unfettered access to and search of mobile device data, including social media content, is not a narrowly tailored government intrusion.²⁵⁹ Such a government intrusion leaves a U.S. citizen's freedom of association and freedom to be anonymous on social media at the whim of CBP officials as experienced by Bikkannavar. Instead, requiring a warrant from a judicial officer provides a balanced approach in weighing the nation security interests of the country with the freedoms of association and anonymity. Otherwise, such an unfettered government intrusion can lead to tyranny and chill a person's political speech on social media, which goes against collective American values and hinders the function of the nation's democracy.²⁶⁰

Thus, warrantless border searches of mobile device data must be narrowly tailored to stave off tyrannical behavior of the government.²⁶¹ One way in which to narrowly tailor the warrantless border search of mobile device data is to simply require CBP officials to obtain a warrant prior to conducting a border search of mobile device data.²⁶² Such a process is more narrowly tailored than a warrantless border search because an independent magistrate can decide, *ex ante*, whether such a border search is constitutional.²⁶³ Having an independent magistrate decide whether the border search is constitutional inherently culls the number of persons whose mobile device data would be subject to a border search by balancing the national security interests of the nation with the

²⁵⁶ Toor, *supra* note 10, at 304; Stein, *supra* note 10, 1256; Allen, *supra* note 1, at 3; Strandburg, *supra* note 1, 747–48; Swire, *supra* note 1, at 1387; Martin & Fargo, *supra* note 5, at 331; Froomkin, *supra* note 5, at 149–50; *NAACP*, 357 U.S. at 460–61; *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 347 (1995).

²⁵⁷ *NAACP*, 357 U.S. at 460–61; *McIntyre*, 514 U.S. at 347; Strandburg, *supra* note 1, at 791; Swire, *supra* note 1, at 1399; Fallon, *supra* note 229, at 1268.

²⁵⁸ *Inspection of Electronic Devices*, *supra* note 15; Motion to Dismiss, *supra* note 44; Iraola, *supra* note 14.

²⁵⁹ *NAACP*, 357 U.S. at 460–61; *McIntyre*, 514 U.S. at 347; *United States v. Montoya de Hernandez*, 473 U.S. 551, 553 (1985).

²⁶⁰ *NAACP*, 357 U.S. at 460–61; *McIntyre*, 514 U.S. at 347; *Montoya de Hernandez*, 473 U.S. at 553; Toor, *supra* note 10, at 321–23; Stein, *supra* note 10, at 1275.

²⁶¹ *Montoya de Hernandez*, 473 U.S. at 553.

²⁶² *Id.*

²⁶³ *Id.* at 552.

freedoms of association and anonymity of the individual.²⁶⁴ Since a warrant must be based on probable cause,²⁶⁵ 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.²⁶⁶ Hence, the pool of potential persons subject to border searches would shrink, thereby “narrowly tailoring” the government intrusion of a border search into the freedoms of association and anonymity, lessening the chilling of political speech.²⁶⁷

CONCLUSION

The freedom of association and freedom to be anonymous of the First Amendment are crucial for a democracy to function in the United States. These rights protect people who are organizing into groups to express protected speech, such as political speech. Further, as technology has evolved, social media has allowed people to organize themselves into informal social media groups or express protected speech anonymously. The freedom of association and the freedom to be anonymous extends to people expressing themselves in informal social media networks or anonymously on social media.

Recent U.S. Supreme Court cases such as *Riley* and *Carpenter* provide constitutional protections for those using social media through mobile devices.²⁶⁸ These cases held that mobile device data that may comprise social media account information includes intimate details of a person’s life as well as political speech expression that should be constitutionally shielded with the greatest of protections from the prying eyes of the government.²⁶⁹ This notion comports with the protection of social media accessible through a mobile device from warrantless border searches by the government under the freedom of association, the freedom to be anonymous, and the Fourth Amendment.²⁷⁰

²⁶⁴ *Id.*

²⁶⁵ *Id.*

²⁶⁶ *Id.*

²⁶⁷ Toor, *supra* note 10, at 327–31; Stein, *supra* note 10, at 1275; POUSTER, BISHOP, & CHWE, *supra* note 251; Allen, *supra* note 1, at 7, 10; Strandburg, *supra* note 1, at 803–04; Swire, *supra* note 1, at 1388; Martin and Fargo, *supra* note 5, at 360–61; Froomkin, *supra* note 5, at 99; *NAACP*, 357 U.S. at 460–61; *McIntyre*, 514 U.S. at 347.

²⁶⁸ *Riley*, 134 S. Ct. at 2484, 2495; *Carpenter*, 138 S. Ct., at 2222–23.

²⁶⁹ Toor, *supra* note 10, at 301; Stein, *supra* note 1, at 1256.

²⁷⁰ Toor, *supra* note 10, at 301; Stein, *supra* note 1, at 1256; POUSTER, BISHOP, & CHWE, *supra* note 251; Allen, *supra* note 1, at 13; Strandburg, *supra* note 1, at 748; Swire, *supra* note 1, at 1388; Martin and Fargo, *supra* note 5, at 313; Froomkin, *supra* note 5; *NAACP*, 357 U.S. at 460–61; *McIntyre*, 514 U.S. at 347.

Thus, as in the real world—in contrast to the cyber world—any government intrusion upon the freedom of association and the freedom to be anonymous in social media groups, including warrantless border searches, is subject to strict scrutiny. Without such a strong shield to protect these rights, the potential government intrusion leads to a silencing of protected speech, hindering the function of democracy. Thus, the government intrusion on the freedom of association and freedom to be anonymous in social media group must be narrowly tailored to a compelling government interest.

Although the government interest of protecting national security from terrorists is a compelling interest, a warrantless border search is not a narrowly tailored government intrusion for this purpose. Instead, a more narrowly tailored government intrusion for this purpose would be obtaining a warrant to search mobile device data. With such a balanced approach in place, it would inherently limit the number of people subject to a mobile device data border search, including their social media, thereby avoiding the obvious consequence of chilling political speech on people's social media that comes with any government intrusion or interference.