MONITORING MIGRANTS IN THE DIGITAL AGE: USING TWITTER TO ANALYZE SOCIAL MEDIA SURVEILLANCE

SUSAN MILLER*

This note uses the collection of social media handles from immigrants, non-immigrants, and other non-citizens by the government as a lens to understand the privacy concerns surrounding social media surveillance and monitoring. This policy also underscores the government's propensity for imposing surveillance techniques that undermine constitutional principles and encroach on constitutionally protected spaces. Against this backdrop, this note analyzes how immigration policy is ill-equipped to ensure constitutional protections in social media surveillance. First, this note will begin with a short history of immigration policies in order to understand why and how government agencies regulate immigration. Next, this note will look at social media surveillance in the domestic and immigration contexts and compare past immigration regulations to the new proposals to show how the nature of social media platforms, coupled with enhanced-surveillance proposals, vastly expand the government's authority. This note will then discuss the constitutional problems and privacy concerns that the social media surveillance regulations pose to immigrants. Finally, this note contends that the collection of social media handles as a form of government surveillance of non-citizens shows how traditional constitutional privacy protections may weaken in digital surveillance contexts.

* J.D., University of Colorado, Class of 2019; B.A., Wellesley College, Class of 2012.

INTRODUCTION 396
I. BACKGROUND ON IMMIGRATION REGULATION 398
A. *Immigration and National Security* 399
B. *Immigration Regulation and Monitoring* 400
II. SOCIAL MEDIA SURVEILLANCE 402
A. *Twitter as a Social Media Platform* 403
B. *Social Media Surveillance in the United States* 405
C. *History of Social Media Surveillance in the Immigration Context* 406
D. *Social Media Surveillance in Comparison with Past Immigration Regulations* 410
III. THE CONSTITUTIONAL CONCERNS WITH SOCIAL MEDIA HANDLE COLLECTION 411
A. *Fourth Amendment: Complications with Open Fields and Third Party Doctrine* 411
1. Is There a Search? 412
a. Open Fields Doctrine 413
b. Third Party Doctrine 414
2. Is the Search Reasonable? 416
B. *First Amendment: Anonymity and Chilling Effects* 417
CONCLUSION 420

INTRODUCTION

Before even setting foot in the United States, non-citizens[1] must provide extensive information in a variety of visa applications.[2] These applications require biographical and personal information such as names, addresses, birthdates, work addresses, job titles, and education information.[3] While this limited type of information has traditionally given the United States Citizenship

1. The term non-citizen in this note will refer to non U.S. citizens who may have either immigrant or nonimmigrant status. Immigrant status refers to those who live permanently in the United States and nonimmigrant status refers to those who are in the United States on a temporary basis. While the terms non-citizen and immigrant will be used interchangeably, these definitions do not include undocumented immigrants, who fall outside the scope of this note. *Nonimmigrant vs. Immigrants Status,* UC BERKELEY: INT'L OFF., https://internationaloffice.berkeley.edu/immigration/nonimmigrantvsimmigrant-status [https://perma.cc/NR6C-NUSC].

2. *See Employment-Based Immigrant Visas,* U.S. DEP'T OF STATE, https://travel.state.gov/content/travel/en/us-visas/immigrate/employment-based-immigrant-visas.html#requireddocs [https://perma.cc/5ENE-2HMC]; *The Immigrant Visa Process*, U.S. STATE DEP'T, https://travel.state.gov/content/travel/en/us-visas/immigrate/the-immigrant-visa-process.html [https://perma.cc/JS46-5AU7] (detailing the forms and process necessary to enter in to the United States as an immigrant).

3. *See Forms,* U.S. CITIZENSHIP & IMMIGR. SERVS., https://www.uscis.gov/forms [https://perma.cc/EZ6H-BHL6] (listing the various forms necessary for various visa categories).

and Immigration Services (USICIS) a rough sketch of a non-citizen's profile, the government has needed to conduct a rigorous background search to fill in finer points. But recent proposals from the Department of Homeland Security (DHS) and the U.S. State Department to collect and store social media handle, coupled with the type of data those handles provide, enable the government to turn that rough sketch into a finely detailed portrait, although it may not be entirely accurate.[4]

These proposals are not the only instances where the government used social media surveillance at the border or for other law enforcement purposes.[5] In 2018, the Florida division of Council on American-Islamic Relations, a Muslim civil rights organization, filed ten complaints with DHS and others regarding enhanced screening of American-Muslim citizens,[6] alleging that the U.S. Customs and Border Protection (CBP) unnecessarily asked questions such as "What social media accounts do you use?" "What is your Twitter account username?" and "What is your Facebook username?"[7] In addition, in early 2017, multiple stories emerged where the government required Muslim Americans, legal permanent residents, and non-immigrant visa holders to hand over social media accounts and passwords to their mobile devices at the border.[8] These examples show the continued encroachment of government surveillance in immigration.

These stories of physical seizures at the border to access social media and the new requirements concerning the collection and storage of social media handles in order to enter the United States are troubling. They not only raise privacy concerns for non-citizens, they also underscore the government's propensity for imposing

4. *See* Notice of Modified Privacy Act System of Records, 82 Fed. Reg. 43,556 (Sept. 18, 2017) [hereinafter *2017 Notice*]; 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, Public Notice 10260, 83 Fed. Reg. 13,807 (Mar. 30, 2018) [hereinafter *2018 Notice*].

5. Sophia Cope & Adam Schwartz, *DHS Should Stop the Social Media Surveillance of Immigrants*, ELECTRONIC FRONTIER FOUND. (Oct. 3, 2017), https://www.eff.org/deeplinks/2017/10/dhs-should-stop-social-media-surveillance-immigrants [https://perma.cc/5PQJ-76S9].

6. Press Release, CAIR-FL, CAIR-FL Files 10 Complaints with CBP After the Agency Targeted and Questioned American- Muslims About Religious and Political Views (Jan. 18, 2017), https://www.cairflorida.org/newsroom/press-releases/720-cair-fl-files-10-complaints-with-cbp-after-the-agency-targeted-and-questioned-american-muslims-about-religious-and-political-views.html [https://perma.cc/9WLT-DP3B].

7. *Id.*

8. Cynthia McFadden et al., *American Citizens: U.S. Border Agents Can Search Your Cellphones*, NBC NEWS (Mar. 13, 2017), http://nbcnews.to/2lU7kkI [https://perma.cc/XXP6-PDEL]; Kaveh Waddell, *A NASA Engineer Was Required to Unlock His Phone at the Border*, ATLANTIC (Feb. 13, 2017), https://www.theatlantic.com/technology/archive/2017/02/a-nasa-engineer-is-required-to-unlock-his-phone-at-the-border/516489/ [https://perma.cc/8XP3-N8MY]; Kaveh Waddell, *'Give Us Your Passwords,'* ATLANTIC (Feb. 10, 2017), https://www.theatlantic.com/technology/archive/2017/02/give-us-your-passwords/516315/ [https://perma.cc/BEY8-AQUM]; Daniel Victor, *What Are Your Rights if Border Agents Want to Search Your Phone?,* N.Y. TIMES, (Feb. 14, 2017), https://nyti.ms/2lgOp1I [https://perma.cc/RV5T-ZKJ4].

surveillance techniques that undermine our constitutional principles and encroach on constitutionally protected spaces when dealing with non-citizens.

Social media is a platform where people can engage in anonymous dialogue, voice dissenting opinions, and engage in political speech.[9] Additionally, the information contained within social media provides the government with the resources to create profiles based on associations due to followers, friends, or location information.

Against that backdrop, this note analyzes how immigration policy is ill-equipped to ensure constitutional protections in social media surveillance. First, this note will begin with a short history of immigration regulation in order to understand why and how government agencies regulate immigration. Next, this note will look at social media surveillance in the domestic and immigration contexts and compare past immigration regulations to the new proposals, to show the nature of social media platforms, coupled with enhanced-surveillance proposals, vastly expand the government's authority. This note will then discuss the constitutional problems and privacy concerns that the social media surveillance regulations pose to non-citizens. Finally, this note argues that these recent immigration proposals weaken Fourth and First Amendment protections for non-citizens.

I. BACKGROUND ON IMMIGRATION REGULATION

Immigration regulation in the United States and the tools authorities have used to regulate immigration have a long and complex history. Indeed, some have asserted that the United States has historically used immigration regulations as a tool to protect national security interests.[10] The use of digital surveillance, such as looking at social media accounts for immigration purposes, comes from the tools that the United States government has developed in order to protect its borders from perceived threats. Social media surveillance and data collection and have also found their way into the toolbox for national security.

9. *See* Rachel K. Brickner, *Tweeting Care: Educators' Dissent through Social Media in the US and Canada*, 77 J. CANADIAN LAB. STUDS 11, 24 (2016) (arguing that dissent through social media is possible through the example of educators on Twitter).

10. *See generally* Arthur L. Rizer III, THE NATIONAL SECURITY IMPLICATIONS OF IMMIGRATION LAW (2012) (contending with an analysis of past laws that the immigration regulations in the United States have been an important means by which to keep adversaries out).

A. *Immigration and National Security*

Almost as soon as the United States formally declared independence from Great Britain, the young nation began to think about how to regulate immigration and national security.[11] In 1882, the Supreme Court established the plenary power doctrine in *Chae Chan Ping v. United States*,[12] where it held that courts may not scrutinize the rules promulgated by the executive or legislative branches regarding immigration regulation.[13] The Supreme Court has since solidified the plenary power doctrine in a number of cases,[14] continually deferring to the political branches in matters concerning non-citizens.

Under this grant of authority, the executive branch has often used immigration regulation to strengthen border security, employing various surveillance techniques.[15] For example, in the McCarran-Walter Act of 1952, the government began excluding immigrants based on political ideology.[16] Although not a form of surveillance itself, this exclusion shows why the government might want to use surveillance in immigration in order to enforce their restrictions.[17] In addition, the government has accumulated surveillance powers in the name of national security, which has given it an outsized view of its power to surveil non-US citizens.[18] Most recently, President Trump has characterized immigration as a national security concern by increasing immigration vetting and adjudications and building a wall at the Mexican border.[19] National

11. *Id.* at 2 (noting that President John Adams exacted the Alien and Sedition Acts in 1798 in order to impose strict naturalization requirements).

12. 130 U.S. 581.

13. *Id.* at 604–07 (holding that Congress and the President of the United States had the exclusive right to exclude immigrants).

14. *See, e.g.*, Mathews v. Diaz et al., 426 U.S. 67 (1976); Kleindienst v. Mandel, 408 U.S. 753 (1972); Galvan v. Press 347 U.S. 522 (1954); Shaughnessy v. U.S. *ex rel.* Mezei, 345 U.S. 206 (1953); U.S. *ex rel.* Knauff v. Shaugnessy, 338 U.S. 537 (1950).

15. *See* Ruchir Patel, *Immigration Legislation Pursuant to Threats to U.S. National Security,* 32 DENV. J. INT'L L. & POL'Y 83, 89–92 (2003) ("Following World War II, the continued fight against Communism reached its peak in the McCarthy Era. This anti-communist sentiment led to the passage of the McCarran-Walter Act of 1952, which introduced an ideological criterion for admission: immigrants and visitors to the U.S. could be denied entry on the basis of their political ideology (e.g., if they were communists)."); Marisa Silenzi Cianciarulo, *Terrorism and Asylum Seekers: Why the REAL ID Act is a False Promise,* 43 HARV. J. ON LEGIS. 101, 113 (2006).

16. *See* Patel, *supra* note 15, at 85; Rizer III, *supra* note 10, at 35 (describing the McCarran-Walter Act of 1952 which allowed the exclusion of aliens based on political ideology, such as Communism).

17. Immigration and Nationality (McCarran-Walter) Act of 1952, Pub. L. No. 82-414, 66 Stat. 163, 184–86 (codified as amended at 8 U.S.C. 1101–1537 (2012)); Exec. Order No. 9066, 7 Fed. Reg. 1407 (Feb. 19, 1942); *see* Patel, *supra* note 15, at 85; Rizer III, *supra* note 10, at 35.

18. *See* Patel, *supra* note 15, at 87–91; Michael F. Dowley, *Government Surveillance Powers Under the USA PATRIOT Act: Is it Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War,* 36 SUFFOLK U. L. REV. 165, 177–78 (2002).

19. *See Immigration*, WHITE HOUSE, https://www.whitehouse.gov/issues/immigration/ [https://perma.cc/5C8E-3DTD]; *National Security & Defense*, WHITE

security has ever been at the forefront of immigration policy but has rarely been defined.[20]

B. *Immigration Regulation and Monitoring*

The immigration policies from the McCarran-Walter Act of 1952 to President Trump's desire to build a border wall, has shown that the United States government conflates immigration and national security which enables the government to use hard-lined surveillance techniques against non-U.S. citizens. On the one hand, the government uses surveillance as part of its national security efforts, such as drones at the border or electronic surveillance under the Foreign Intelligence Surveillance Act (FISA).[21] On the other hand, the United States government also regularly collects various identifying pieces of data for non-citizens entering the country as part of its routine immigration procedure.[22] This information is necessary to ensure public safety and national security by excluding potential threats based on the information provided in the visa forms.[23] For example, a non-immigrant worker visa application typically asks for information such as full legal name, passport number, foreign and U.S. mailing address.[24]

In addition, for someone wishing to join their U.S. citizen spouse legally in the U.S., the government requires similar identifying information plus greater evidence of the relationship with the U.S. citizen such as leases, documents showing combined financial resources, and affidavits from third parties recognizing the marriage as valid.[25] The government has various reasons for

---

HOUSE, https://www.whitehouse.gov/issues/national-security-defense/ [https://perma.cc/PD8A-3CVJ]; *President Donald J. Trump Announces Enhanced National Security Measures*, WHITE HOUSE, (Sept. 24, 2017), https://www.whitehouse.gov/the-press-office/2017/09/24/president-donald-j-trump-announces-enhanced-national-security-measures [https://perma.cc/HPS7-DEMW].

20. *See* Rizer III, *supra* note 10, at 49 (stating that President George W. Bush believed national security to encompass the economy and military interests of the United States whereas President Barack Obama saw national security interests as the security of the citizens of the United States and the security of its allies and partners).

21. Michael Avery, *The Constitutionality of Warrantless Electronic Surveillance of Suspected Foreign Threats to the National Security of the United States*, 62 U. MIAMI L. REV. 541, 549 (2008) ("FISA regulates electronic surveillance for foreign-intelligence and national-security purposes within the United States."); Matt Novak, *U.S. Border Patrol Flew More Drone Missions Last Year Than Ever Befo*re, GIZMODO (Sept. 26, 2018, 10:30 AM), https://gizmodo.com/u-s-border-patrol-flew-more-drone-missions-last-year-t-18293 23612 [https://perma.cc/2RYC-R57X].

22. *Checklist of Required Initial Evidence for Form 1-485 (for Informational Purposes Only)*, U.S. CITIZENSHIP & IMMIGR. SERVS., https://www.uscis.gov/i-485Checklist [https://perma.cc/CL4J-NEGJ] (last updated Sept. 10, 2018); *H-1B Checklists for New and Extension Petitions*, U. WASH., https://ap.washington.edu/ahr/visas/h1b/checklists/ [https://perma.cc/3EZJ-P6FH].

23. Anil Kalhan, *Immigration Surveillance*, 74 MD. L. REV. 1, 13 (2014).

24. *I-129, Petition for Nonimmigrant Worker*, U.S. CITIZENSHIP & IMMIGR. SERVS., https://www.uscis.gov/i-129 [https://perma.cc/JV2E-YZH5].

25. *I-130, Petition for Alien Relative*, U.S. CITIZENSHIP & IMMIGR. SERVS., https://www.uscis.gov/i-130 [https://perma.cc/HH6S-Q86C].

obtaining this information including ability to contact the non-citizen, compliance with immigration regulations, preventing fraud, and ensuring eligibility.[26]

Although this information is useful for visa approval, this data—U.S. address, email address, and employment details, etc.—enables the government to start building out profiles, which it can then use to contact and monitor non-citizens after they enter in the U.S. In the past, collection of this information has been somewhat innocuous, but with the rise of social media surveillance, the government can now create a more robust profile based on even one social media handle.

Anil Kalhan noted in *Immigration Surveillance* that noncitizens are "scrutinized more closely than ever before" through visa applications, during their travel, and at the border.[27] Kalhan also described the trend toward the monitoring of noncitizens after entry into the U.S. Whereas in the past, scrutiny at the border was the main immigration enforcement mechanism, continued monitoring enables the government to track and deport noncitizens who overstay their visa or for post-entry criminal conduct.[28] Examples include the continued monitoring of international students through the Student and Exchange Visitor Information System and the use of systems such as the Systematic Alien Verification for Entitlements program by federal and local agencies to verify immigration status for public benefits.[29] Section II.C. will elaborate further on social media surveillance in immigration.

While the U.S. government has legitimate reasons for enforcing and monitoring noncitizens, it is important to note that noncitizens are not without rights. Noncitizens, once inside the U.S., share many of the same protections guaranteed by the Constitution as citizens, such as due process and equal protection.[30] For example, the equal protection clause of the Fourteenth Amendment, the due process clause of the Fifth Amendment, and the Fourth Amendment's guarantees all apply to noncitizens within the U.S.[31] Additionally, the First Amendment applies to non-

26. *Volume 2, Part J, Chapter 6 – Adjudication, Policy Manual*, U.S. CITIZENSHIP & IMMIGR. SERVS., https://www.uscis.gov/policymanual/HTML/PolicyManual-Volume2-PartJ-Chapter6.html [https://perma.cc/Q762-B5WC]; *Volume 8, Part J, Chapter 3 – Adjudicating Inadmissibility*, U.S. CITIZENSHIP & IMMIGR. SERVS., https://www.uscis.gov/policymanual/HTML/PolicyManual-Volume8-PartJ-Chapter3.html#S-C [https://perma.cc/QA2S-RSBY].

27. Kalhan, *supra* note 23, at 14–18.

28. *Id.* at 17–18.

29. *Id.* at 47–48, 51.

30. Louis Henkin, *The Constitution as Compact and as Conscience: Individual Rights Abroad and at Our Gates*, 27 WM. & MARY L. REV. 11, 13–18 (1985). This Note does not address the rights of undocumented immigrants.

31. Marisa Antos-Fallon, *Privacy and Immigration Enforcement*, 35 FORDHAM URBAN L.J. 999, 1015 (2008) ("First, the language of the Fourth Amendment extends to non-citizens, and courts have repeatedly recognized this, weighing the Fourth

citizens as well.[32] However, some Congressional imposed distinctions between noncitizens and citizens have been found reasonable, such as excluding noncitizens from political activities, such as voting.[33] Finally, although some protections may exist extraterritorially, noncitizens outside of the U.S. seeking entry have fewer guarantees.[34]

II. SOCIAL MEDIA SURVEILLANCE

The rise of technology in general, and the rise of social media platforms in particular, has led to complicated regulatory and legal dilemmas.[35] While the plenary power doctrine enables the government to have a broad authority in dealing with national security, the digital collection of data also enables the government to create and draw detailed profiles of non-citizens. This even puts non-citizens in a position where they might be monitored even after their profile is created and once they are in the United States. The use of social media surveillance in modern immigration regulation is best understood by looking at what constitutes a social media platform, the history of social media surveillance, and comparing this surveillance to past immigration regulations. While many examples of social media platforms exist,[36] this Note will use Twitter, a seemingly innocuous social media platform, to highlight these themes.

Amendment interests of non-citizens in evaluating the constitutionality of immigration enforcement action."); *id.* at 16.

32. Michael Kagan, *Do Immigrants Have Freedom of Speech*?, 6 CAL. L. REV. 83, 92 (2015) ("Finally, the Supreme Court has at least twice said that the First Amendment applies to non-citizens in the country. In Bridges v. Wixon, the Court said, 'Freedom of speech and of press is accorded aliens residing in this country.'").

33. *Id.* at 94; Zoë Robinson, *Constitutional Personhood*, 84 GEO. WASH. L. REV. 605, 638–39 (2016).

34. Henkin, *supra* note 30, at 26–27 (discussing a number of lower court decisions that recognize constitutional protections for noncitizens in specific contexts); Kevin R. Johnson, *Immigration and Civil Rights in the Trump Administration: Law and Policy Making by Executive Order*, 57 SANTA CLARA L. REV. 611, 648 (2017); Timothy Zick, *The First Amendment in Trans-Border Perspective: Toward A More Cosmopolitan Orientation*, 52 B.C.L. REV. 941, 975 (2011) ("Courts and commentators, however, have generally been skeptical that aliens located abroad enjoy free speech protections."); *see* Lyle Denniston, *Constitution Check: Do Individual Rights Stop at the U.S. Border?* CONST. DAILY (Oct. 29, 2015) https://constitutioncenter.org/blog/constitution-check-do-individual-rights-stop-at-the-u-s-border/ [https://perma.cc/D8BD-MYWL] (discussing the application of the Constitution abroad to noncitizens).

35. *See* Marissa Kazemi, *Families of Pulse Nightclub Victims Face Off Against Twitter, Facebook and Google*, 94 DENV. L. REV. ONLINE 1, 1–3 (2017) (discussing how most social media companies are immune under Section 2030 from internet trolls but what internet companies themselves might do to curb online abuse). *See generally* F. Cassim, *Formulating Adequate Legislation to Address Cyber-Bulling: Has the Law Kept Pace with Advancing Technology*, 26 S. AFR. J. CRIM. JUST. 1 (2013) (discussing the rise of cyberbullying and possible regulatory solutions in South Africa).

36. *Social Media Platforms*, DELVALLE INST., https://delvalle.bphc.org/mod/wiki/view.php?pageid=65 [https://perma.cc/SSD8-FLLA] (listing Facebook, Google+, LinkedIn, Twitter, Tumblr, Instagram, Pinterest, and Snapchat as examples of various forms of social media).

A. *Twitter as a Social Media Platform*

What is social media? While definitions vary, most assume that social media is some type of application that permits users to interact with one another by sharing information or content.[37] It is used across the globe to connect family, friends, acquaintances, and strangers. A variety of social media platforms exist to connect people with various shared interests. Social media accounts can be accessed over web browsers on laptops or via apps on tablets and smartphones. Social media accounts are a new form of communication that allow for information sharing far beyond that of a traditional phone call. This Note will focus on one currently popular platform: Twitter. Twitter provides a particularly pointed example to analyze social media surveillance because of its unique characteristics as a social media platform such as its handles, personal pages, limited viewing settings, and metadata. This section will set the stage for why Twitter is a good social media platform through which to analyze the constitutional concerns discussed in Part III infra.

Specifically, unlike other social media profiles, such as Facebook which requires the user to use their real name, Twitter allows the user to create pseudonymous accounts. While the user must use a full name to initially sign up for the account along with an email address, the name viewed publicly can be a pseudonym.[38] Twitter allows the user to have a profile set to "public" or "private."[39] If the user does not limit the account to a more private setting, public posts on Twitter may be viewed by anyone, registered with Twitter or not.[40] Twitter users can follow any other accounts that they wish to in order to view other posts in their

37. *Social Media,* OXFORD REFERENCE: A DICTIONARY OF MEDIA AND COMMUNICATION (2d ed. 2016), http://www.oxfordreference.com/view/10.1093/acref/9780191800986.001.0001/acref-9780191800986-e-2539 [https://perma.cc/337B-ZQSK] ("A broad category or genre of communications media which . . . enable[s] social interaction among groups of people, . . .[s]uch media can be thought of metaphorically as virtual meeting places which functions to occasion the exchange of media content among users who are both producers and consumers."); Vanessa S. Browne-Barbour, *A Fork in the Road: The Intersection of Virtual Law Practice and Social Media*, 52 WASHBURN L.J. 267, 275 (2013) ("'[S]ocial media is a catch phrase that describes technology that facilitates interactive information, user-created content and collaboration.'") (quoting Carolyn Elefant, *The "Power" of Social Media: Legal Issues & Best Practices for Utilities Engaging in Social Media*, 32 ENERGY L.J. 1, 4 (2011)).

38. *See How to Control Your Data on Twitter*, ME & MY SHADOW (June 15, 2016), https://myshadow.org/how-to-increase-your-privacy-on-twitter [https://perma.cc/TR3H-5EG2] (providing tips to increase anonymity such as using a different email address not linked to other accounts and a pseudonym instead of your real name); *Signing up with Twitter*, TWITTER, https://help.twitter.com/en/create-twitter-account [https://perma.cc/7PXS-M7SR].

39. *About Public and Protected Tweets*, TWITTER, https://help.twitter.com/en/safety-and-security/public-and-protected-tweets [https://perma.cc/ZX49-AMLF].

40. *Id.*

feed.[41] While some anonymous Twitter users might hide for nefarious reasons, such as trolling,[42] others use pseudonyms for protecting reputations or personal safety.[43]

Perhaps most relevant here though, often those who choose to use pseudonyms might be whistleblowers, dissenters, or someone wishing to express their viewpoint without personal repercussions.[44] The ability to engage in conversation with other users, use pseudonymous accounts, and follow various news sources, permit users of Twitter to be part of a curated, online community.

In addition to the First Amendment issues, the unique features of Twitter also create unique challenges in privacy protections because of the collection of data and surveillance of anonymous profiles. Although Section III.A will provide an in depth analysis of how Twitter implicates the Fourth Amendment, briefly, courts have historically recognized that the Fourth Amendment protects content of a letter but not the information on the envelope containing the letter.[45] While at first glance, the Twitter handle itself may appear to be merely envelope material and the information on the page appears closely related to content. The pseudonymous nature of a Twitter and the differences between public and potentially private posts poses possible hurdles, in addition to the problems that metadata present.

In short, Twitter offers a variety of uses that range from personal marketing to digital citizenship to anonymous conversations. The various uses and privacy functions of Twitter create a complex policy question regarding their surveillance, which will be examined after discussing domestic and immigration social media surveillance. The following sections will establish context for the later privacy discussions surrounding Twitter and immigration by discussing how social media muddles historical legal analysis.

---

41. *How to Follow People on Twitter*, TWITTER, https://help.twitter.com/en/using-twitter/how-to-follow-someone-on-twitter [https://perma.cc/QR6W-S7BG].

42. Andre Bourque, *Answering a Social Troll – What You Need to Know*, HUFFINGTON POST, https://www.huffingtonpost.com/andre-bourque/answering-a-social-troll_b_6625654.html [https://perma.cc/8RJA-K82Q] (updated Dec. 6, 2017).

43. Judith S. Donath, *We Need Online Alter Egos Now More Than Ever*, WIRED (Apr. 25, 2014), https://www.wired.com/2014/04/why-we-need-online-alter-egos-now-more-than-ever/ [https://perma.cc/Y3H7-GE6N]; *Who Is Anonymous on Twitter? Six Common Reasons People Don't Use Their Real Names*, ONLINE ACAD. (Dec. 17, 2014), https://onlineacademic.wordpress.com/2014/12/17/who-is-anonymous-on-twitter/ [https://perma.cc/G8KY-4RSN].

44. Brooke Binkowski, *Twitter's Alts and Rogues*, SNOPES (Apr. 24, 2018), https://www.snopes.com/news/2017/06/01/alts-and-rogues/ [https://perma.cc/AD2S-EL6N].

45. *See ex parte* Jackson, 96 U.S. 727, 733 (1877) (holding that sealed letters and packages sent through the post office cannot be opened without a warrant); *see also* Smith v. Maryland, 442 U.S. 735 (1979) (distinguishing between the privacy of phone conversations from the privacy of the numbers dialed on a telephone).

B. *Social Media Surveillance in the United States*

To understand how the government uses Twitter, it is important to understand the legal framework for social media surveillance more broadly. Although perhaps shocking to some of the American public, using social media as a means of surveillance is not unique to immigration policy. For example, in 2010, it was revealed that law enforcement agencies were considering using social media surveillance in several situations.[46] Indeed, in the disclosures, the CIA revealed that their "Open Source Center," the center that analyzes open source material, had been collecting publicly available social media information from social media platforms since 2005.[47] In order to monitor, law enforcement use social media monitoring software such as GeoFeedia, a tool that analyzes location information and social media information, even when social media data is supposedly being protected by privacy settings.[48]

Although in some situations surveillance is beneficial, overall, it has enabled the government to amass a tremendous amount of data. Indeed, the government views social media intelligence gathering as a particularly important tool for counterterrorism efforts, such as to gather information on ISIS fighters.[49] Additionally, reports have surfaced that law enforcement has used social media to address potential crime during the U.S. Open of Surfing.[50] These instances illustrate the government's interest in using social media surveillance to find members of various associations, gather location information, and establish crimes.[51] However, the government's use of social media to surveil creates

46. *See, e.g.*, U.S. DEP'T OF JUSTICE, CRM-200900732F, OBTAINING AND USING EVIDENCE FROM SOCIAL NETWORKING SITES (2010) [hereinafter DOJ SOCIAL NETWORK PRESENTATION], https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf [https://perma.cc/FBJ8-KKZJ] (presentation by DOJ on social network surveillance, how to obtain data with the phrase "Undercover operations?" as a possibility); LAUREN WAGNER, USING THE MYSPACE FRIEND MAPPER TO BUILD CONNECTIONS FOR AN INVESTIGATION (Oct. 2007), https://www.eff.org/files/filenode/myspace_friend_mapper_article_2007.pdf [https://perma.cc/74Q8-ADGC] (describing how the Friend Mapper tool, once created "for fun," can be useful for law enforcement by allowing investigators to "[b]uild[] connections to a person that might not have been available by just viewing that person's top friends" or "[p]rovide a useful diagram that can be added to a case file and used in court"); Jennifer Lynch, *Government Finds Uses for Social Networking Sites Beyond Investigations*, ELECTRONIC FRONTIER FOUND. (Aug. 10, 2010), https://www.eff.org/deeplinks/2010/08/government-finds-uses-social-networking-sites [https://perma.cc/HF7X-WU29] (stating that the disclosures revealed that social media was being considered for background checks and security clearances).

47. Lynch, *supra* note 46.

48. Chris Bousquet, *Mining Social Media Data for Policing, the Ethical Way,* GOV'T TECH. (Apr. 27, 2018), http://www.govtech.com/public-safety/Mining-Social-Media-Data-for-Policing-the-Ethical-Way.html [https://perma.cc/Y4XP-5M32].

49. Hugh Handeyside, *To the Government, Your Latest Facebook Rant Is Raw Intel*, ACLU (Sept. 29, 2016), https://www.aclu.org/blog/privacy-technology/internet-privacy/government-your-latest-facebook-rant-raw-intel [https://perma.cc/WH6U-N4VH].

50. Bousquet, *supra* note 48.

51. *See, e.g.*, DOJ SOCIAL NETWORK PRESENTATION, *supra* note 46.

constitutional concerns, such as freedom of speech and association, when such surveillance leads to racial targeting and greater scrutiny of individuals based on a single post.[52] For example, Memphis police monitored and collected information on Black Lives Matter supporters via Facebook,[53] and the Boston Police Department targeted the hashtag #MuslimLivesMatter.[54]

Against that backdrop, it is of little surprise that similar surveillance might be considered beyond local law enforcement, especially given the government's history of using immigration as a way to protect the border. What is more concerning, however, is when the government surveils the social media profiles—and relevant here, the Twitter handles—of non-citizens.

C. *History of Social Media Surveillance in the Immigration Context*

The fact that the DHS, like other law enforcement agencies, collects social media information is not new.[55] While not tied specifically to immigration, the DHS began collecting social media data as early as 2010, supposedly in order to better track disasters because social media could provide public reports that could be used in comprehensive report on breaking events.[56] Since 2015, the DHS, USCIS, and ICE have continued to expand social media surveillance in connection with those seeking U.S. immigration status or non-immigrant visas.[57]

For example, in the fall of 2016, CBP officers began to gather information from social media profiles during the Electronic System for Travel Authorization (ESTA) application process.[58] ESTA is a

52. Handeyside, *supra* note 49.

53. Antonia Noori Farzan, *Memphis Police Used Fake Facebook Account to Monitor Black Lives Matter, Trial Reveals*, WASH. POST (Aug. 23, 2018), https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/?utm_term=.4c3ea8cf36c2 [https://perma.cc/J6RF-A85G].

54. *Report: Boston Police Social Media Monitoring Targeted Muslims, Black Lives Matter Posts*, WCVB, https://www.wcvb.com/article/boston-police-black-lives-matter-racial-inequality-muslim-lives-matter-social-media/16751692 [https://perma.cc/YCR9-CTX6] (updated Feb. 7, 2018).

55. Cope & Schwartz, *supra* note 5.

56. *DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism & Intelligence of the H. Comm. on Homeland Sec.*, 112th Congress 12–16 (2012) (joint prepared statement by Mary Ellen Callahan, Chief Privacy Officer, Department of Homeland Security, & Richard Chávez, Director, Office of Operations Coordination and Planning, Department of Homeland Security).

57. *See* DEP'T OF HOMELAND SEC., OIG-17-40, DHS' PILOTS FOR SOCIAL MEDIA SCREENING NEED INCREASED RIGOR TO ENSURE SCALABILITY AND LONG-TERM SUCCESS (2017); DEP'T OF HOMELAND SEC., IA-900, OFFICIAL USAGE OF PUBLICLY AVAILABLE Information (2015).

58. Edward Helmore, *US Government Collecting Social Media Information from Foreign Travelers*, GUARDIAN (Dec. 26, 2016), https://www.theguardian.com/world/2016/dec/26/us-customs-social-media-foreign-travelers [https://perma.cc/5NNH-PUJ6].

process where citizens from Visa Waiver Countries, such as Japan, the United Kingdom, and Chile, submit their data to an electronic system that verifies eligibility to travel to the United States.[59] Part of this verification is whether there are security risks if the traveler enters the United States.[60] The CBP assures applicants that the social media information will be used to "enhance the vetting process" and possibly to "validate legitimate travel . . . and identify potential threats."[61] Additionally it states that it would only look into publicly available social media information in a way "consistent with the privacy settings the applicants have set on the platforms."[62] However, digital surveillance policies could lead to the invasive surveillance of social media data, cloud data, and other information that may or may not be public.[63] Indeed, in 2017, then-U.S. Homeland Security Secretary John Kelly proposed that DHS should require people visiting the United States to hand over social-media passwords as part of enhanced security checks.[64]

Shortly thereafter, the DHS issued the Notice of Modified Privacy Act System of Records ("2017 Notice"), which stated that the DHS planned to collect personal information from immigrants social media profiles and store it in their already existing Alien File ("A-File"), a profile that contains more routine biographical information.[65] In March 2018, the State Department issued a Notice of Proposed Information Collection ("2018 Notice"), which would expand its efforts to collect information from nonimmigrants

59. Sophia Cope, *U.S. Customs and Border Protection Wants to Know Who You Are on Twitter—But It's a Flawed Plan,* ELECTRONIC FRONTIER FOUND. (Aug. 22, 2016), https://www.eff.org/deeplinks/2016/08/us-customs-and-border-protection-wants-know-who-you-are-twitter-its-flawed-plan [https://perma.cc/VTR4-7CF3].

60. *Official ESTA Application*, U.S. CUSTOMS & BORDER PROTECTION, https://esta.cbp.dhs.gov/esta/ [https://perma.cc/3D29-367R].

61. *Frequently Asked Questions, Social Media*, U.S. CUSTOMS AND BORDER PROTECTION, https://esta.cbp.dhs.gov/esta/application.html?execution=e2s1 [https://perma.cc/SV57-2EKP].

62. Iain Thomson*, Will US Border Officials Demand Social Network Handles from Visitors?*, REGISTER (Sept. 21, 2016), https://www.theregister.co.uk/2016/09/21/want_to_visit_the_land_of_the_free_then_customs_will_demand_social_media_accounts/ [https://perma.cc/9UPB-5UQE].

63. *See* Electronic Frontier Found., Comment Letter on Proposed Collection of Social Media Identifiers via Arrival and Departure Record (Forms I–94 and I–94W) and Electronic System for Travel Authorization States (Aug. 22, 2016), https://www.regulations.gov/contentStreamer?documentId=USCBP-2007-0102-0596&attachmentNumber=1&contentType=pdf [https://perma.cc/GC85-VXFN].

64. Alexander Smith, *U.S. Visitors May Have to Hand Over Social Media Passwords: DHS,* NBC NEWS (Feb. 8, 2017, 7:51 AM), https://www.nbcnews.com/news/us-news/amp/us-visitors-may-have-hand-over-social-media-passwords-kelly-n718216 [https://perma.cc/749P-V469] ("'We want to get on their social media, with passwords: What do you do, what do you say?' he told House Homeland Security Committee. 'If they don't want to cooperate then you don't come in.'").

65. *2017 Notice*, *supra* note 4 (clarifying that the system covers "[l]awful permanent residents; Naturalized U.S. citizens; Individuals when petitioning for benefits under the INA, as amended, on behalf of another individual; Individuals acting as legal guardians or designated representatives in immigrant proceedings involving an individual who has a physical or developmental disability or mental impairment . . ." among others).

social media accounts by requiring visa applicants to submit social media identifiers from the past five years.[66] In the 2018 Notice, the State Department noted that the collection of social media handles is merely for "identity resolution and vetting purposes based on statutory visa eligibility standards."[67] The form proposed to collect social media information is the DS-160 which is required for nearly all nonimmigrant visas such as business, student, fiancée, or work.[68] The DS-160 collects biographical information such as family names, spouse information, education, and work history.[69]

As surveillance measures for immigrants become more extensive, an important question to ask is why the DHS wants to collect information from social media in the first place? One hypothesis is that the DHS gathers data from social media as an effort to combat national security threats and counterterrorism.[70] For example, lawmakers urged the DHS to gather data from the social media accounts of visa applicants because they were concerned that the government was missing an opportunity to prevent mass shootings after the San Bernardino shooting by two permanent residents in 2015.[71]

Under the 2017 Notice, the DHS wants to collect social media data, but Twitter poses a particularly difficult problem. As discussed in Section II.A, Twitter allows users to create pseudonymous accounts.[72] More specifically, but for a DHS request, a Twitter handle cannot be easily connected to its user. Some might argue that immigrants seeking entry could just not disclose anonymous Twitter handles. However, the implications of not disclosing such accounts are life changing for those seeking to enter should the government determine willful nondisclosure is equivalent to willful misrepresentation. [add a sentence like "Indeed, an immigrant could be banned indefinitely from the

66. *2018 Notice, supra* note 4; Tal Kopan*, US to Require Would-Be Immigrants to Turn Over Social Media Handles*, CNN: POLITICS (Mar. 29, 2018) https://www.cnn.com/2018/03/29/politics/immigrants-social-media-information/index.html [https://perma.cc/GG8C-HWEY].

67. *2018 Notice, supra* note 4.

68. *DS-160: Frequently Asked Questions*, U.S. DEP'T STATE – BUREAU OF CONSULAR AFF., https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/forms/ds-160-online-nonimmigrant-visa-application/ds-160-faqs.html [https://perma.cc/562Y-4T6T]; *Online Nonimmigrant Visa Application (DS-160),* U.S. DEP'T STATE, https://travel.state.gov/content/dam/visas/PDF-other/DS-160_Example.pdf [https://perma.cc/MVP8-CPDU].

69. *Online Nonimmigrant Visa Application (DS-160)*, *supra* note 68.

70. Evan Perez & Dana Ford, *San Bernadino Shooter's Social Media Posts on Jihad Were Obscured*, CNN (Dec. 14, 2105), http://www.cnn.com/2015/12/14/us/san-bernardino-shooting/index.html [https://perma.cc/Q5XK-J8US] (discussing the shooting by Tashfeen Malik and her husband Syed Rizwan Farook that killed 14 people where Ms. Malik discussed jihad in a private online chat).

71. Ron Nixon, *U.S. to Collect Social Media Data on All Immigrants Entering Country*, N.Y. TIMES (Sept. 28, 2017), https://nyti.ms/2fChbtx [https://perma.cc/Z77T-MT8Q].

72. *Supra* Section II.B.

United States" or something like that to explain the "life changing" outcome.[73]

Additionally, by collecting social media handles from Twitter, the DHS will be able to collect more personal information than ever before, information that provides an "intimate window into a person's life."[74] Not only will names, birthdates, and addresses be on the record, but also photos, connections, tweets the user has liked or commented on, and other historical location data.[75] Much of this data will go back years, musings posted almost a decade ago can now come back to haunt someone wishing to enter the United States.[76] While writing down a Twitter handle on an immigration form may feel like jotting down an address, an example of envelope information,[77] the amount of information that can later be obtained through vetting and future monitoring from this one piece of envelope information is concerning. The inferences that can be deduced from the vast amounts of information available after a social media handle is turned over begins to appear more like content information.

The current 2017 Notice and 2018 Notice would therefore expand previous social media surveillance.[78] While the 2018 Notice and the revised 2016 ESTA application indicate that the social media handles will be used for vetting prior to entering the country, once that information is in the system the use becomes less clear.

---

73. *See Chapter 2 – Overview of Fraud and Willful Misrepresentation,* U.S. CITIZENSHIP & IMMIGRATION SERVS., https://www.uscis.gov/policymanual/HTML/PolicyManual-Volume8-PartJ-Chapter2.html [https://perma.cc/N9D9-5F6G] (stating that an applicant will be inadmissible if they obtain entry through fraud or willful misrepresentation); *see also* U.S. CITIZENSHIP AND IMMIGRATION SERVS., PM-602-0163, ISSUANCE OF CERTAIN RFES AND NOIDS; REVISIONS TO *ADJUDICATOR'S FIELD MANUAL (AFM)* CHAPTER 10.5(A), CHAPTER 10.5(B) (2018), https://www.uscis.gov/sites/default/files/USCIS/Laws/Memoranda/AFM_10_Standards_for_RFEs_and_NOIDs_FINAL2.pdf [https://perma.cc/8GCV-7FKM]; Graham Kates, *Changes to Federal Policies Pave Way for Sudden Visa Denials, Deportation*, CBS NEWS (July 19, 2018), https://www.cbsnews.com/news/changes-to-federal-policies-pave-way-for-sudden-visa-denials-deportation/ [https://perma.cc/HJ9A-E2QH].

74. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

75. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089–91 (2002). Though outside the scope of this note, the 2017 Notice also aimed to "update record source categories to include publicly available information obtained from. . . commercial data providers." *2017 Notice, supra* note 4; Violet Blue, *Americans Are Horrified by DHS Plan to Track Immigrants on Social Media*, ENGADGET:B@D P@SSW0RD (Sept. 29, 2017), https://www.engadget.com/2017/09/29/dhs-to-track-immigrants-on-social-media/ [https://perma.cc/QM3U-92A6].

76. See Sam Wolfson, *New York Times Racism Row: How Twitter Comes Back to Haunt You*, GUARDIAN (Aug. 3, 2018), https://www.theguardian.com/technology/2018/aug/03/sarah-jeong-new-york-times-twitter-posts-racism?CMP=share_btn_tw [https://perma.cc/3U28-ZKKX] (discussing Sarah Jeong's satirical tweets which resurfaced and labeled as racist against white people when she was hired by the New York Times).

77. *See supra* Section II.A.

78. Sophia Cope & Adam Schwartz, *DHS Should Stop the Social Media Surveillance of Immigrants*, ELECTRONIC FRONTIER FOUND. (Oct. 3, 2017), https://www.eff.org/deeplinks/2017/10/dhs-should-stop-social-media-surveillance-immigrants [https://perma.cc/DY24-KJAJ].

Indeed, the examples of social media monitoring at the U.S. Open Surfing Competition and of the Black Lives Matter movement mentioned in Part II.B. show that monitoring, not just vetting, can and will occur.[79]

D. *Social Media Surveillance in Comparison with Past Immigration Regulations*

Vetting immigrants by the United States government is not a new practice. The reach of broad social media surveillance is. Under the plenary power doctrine, the executive and legislative branches have enacted immigration regulations that define reasons for deportation and requirements for entry. Since 1798 it has not been an easy process to immigrate to the United States, often due to the restrictions put in place. Like earlier forms of surveillance or restrictions such the McCarran-Walter Act of 1952, the use of social media surveillance aims to vet out "unwanted" immigrants. Searching social media for connections to extremist organizations or posts about criminal behavior may fall in line with immigration policies to ensure a safer country. However, the vast majority of information that can be searched on social media accounts, such as Twitter, will not be related to anything dangerous, but rather will be closer to reading a diary, a planner, or a photo album. While immigrants may expect a greater amount of scrutiny in order to enter the United States, the collection of a large amount of information unrelated to the requirements of a visa application pose privacy concerns which will be discussed in the next section.

Additionally, the collection of social media handles may seem as innocuous as collecting one's name or birthdate. Indeed, the government's reasoning for collecting social media handles could be seen as another form of collecting identifiers or other necessary information required for non-immigrant work visas or green card applications. However, the government is likely not collecting social media handles to send visas to recipients over Twitter. Instead, due to their social media surveillance history, the DHS requests social media for the information that could possibly be extrapolated from the account itself. Thus, while a social media handle may seem like just a name or other identifier, the ability to collect vast amounts of information from Facebook and Twitter raises some complicated constitutional concerns.

---

79. *See, e.g.*, Chantal Da Silva, *ICE Just Launched a $2.4M Contract with a Secretive Data Surveillance Company that Tracks You in Real Time*, NEWSWEEK (June 7, 2018), https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493 [https://perma.cc/NT3K-QQ45].

III. THE CONSTITUTIONAL CONCERNS WITH SOCIAL MEDIA HANDLE COLLECTION

That the DHS through USCIS is collecting and storing social media handles—and, relevant here, Twitter handles—raises privacy concerns under both the Fourth and First Amendment.[80] Indeed, this note evaluates how the DHS's new policy, in using social media surveillance in monitoring noncitizens, likely harms immigrants' reasonable expectations of privacy and could cause a chilling effect. Even if not legally cognizable, long term ramifications exist. While the government may have authority under the plenary power doctrine in the interest of national security, sweeping social media surveillance, especially in sustained monitoring, weakens the expectation of privacy for immigrants.[81]

A. *Fourth Amendment: Complications with Open Fields and Third Party Doctrine*

The Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated"[82] and has traditionally been a guarantee of the protection of property from invasive government searches.[83] However, courts have extended Fourth Amendment protections beyond invasions of tangible effects.[84] The collection of Twitter handles also raises new Fourth Amendment concerns due to the nature of information contained beyond the handle itself.

In *Katz v. United States*,[85] the Supreme Court clarified how privacy is protected under the Fourth Amendment, stating that "the Fourth Amendment protects people, not places."[86] The Court in *Katz* held that wiretapping public telephone booths constituted a search and required a warrant, paving a way for protections of intangible intrusions rather than just physical trespass of the sort

80. *See* Louis Henkin, *The Constitution As Compact and As Conscience: Individual Rights Abroad and at Our Gates*, 27 WM. & MARY L. REV. 11, 16 (1985); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 722 cmt. a (AM. LAW. INST. 1987) ("The Bill of Rights of the United States Constitution (Amendments I-X) declares the rights of persons, not of citizens only. Aliens in the United States therefore enjoy, notably, the freedoms of speech, press, religion, and assembly (Amendment I), the rights of privacy and freedom from unreasonable arrest and search or seizure (Amendment IV) . . . .").

81. *See supra* Section I.B.

82. U.S. CONST. amend. IV.

83. Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection,* 11 UCLA J.L. & TECH. 1, 8 (2007).

84. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

85. 389 U.S. 347 (1967).

86. *Id.* at 351.

enumerated in the Fourth Amendment.[87] In order to determine the constitutional implications of the collection Twitter handles, this note asks the questions (1) is there a search; and (2) is the search reasonable?[88] By analyzing the collection of Twitter handles, especially pseudonymous handles, this note will show that in some instances a mass collection of social media handles threatens the protections afforded by the Fourth Amendment.

1. Is There a Search?

The collection of Twitter handles may not seem like a traditional search under the Fourth Amendment. According to Justice Harlan's reasonable expectation of privacy test in *Katz v. United States*, courts determine if there is a search by asking (1) does a person have an actual or subjective expectation of privacy, and (2) is that expectation one that society would recognize as reasonable.[89] *Katz* created the reasonable expectation of privacy test that federal courts continue to use.[90] Applying this test to pseudonymous Twitter handles underscores the problem with applying the Fourth Amendment to digital content.

Other social media profiles such as Facebook, for example, require an individual's real name and would likely fail to satisfy the first question, since courts have held that there is no seizure when there is a request for identification.[91] Twitter, on the other hand, handles might contain a full legal name, but they can just as easily be a pseudonym.[92] Thus, pseudonymous Twitter accounts raise three issues separate from Facebook accounts using real names.

These three issues under the "is it a search" question include first, can there still be a reasonable expectation of privacy under the open field doctrine when the information is shared with the public? Second, certain information is held by the ISP, or Twitter. How might there still be a reasonable expectation of privacy in information shared with ISPs by anonymous accounts? Finally, the anonymity of Twitter handles raises freedom to associate implications.

87. *Id.* at 353–56.

88. DANIEL SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 256 (2018).

89. *Katz*, 389 U.S. at 351.

90. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring); Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places*, 16 VA. J.L. & TECH. 430, 439 (2011).

91. Gilmore v. Gonzales, 435 F.3d 1125, 1137–38 (9th Cir. 2006) (holding that the request for identification policies such as presenting identification before boarding an airplane is not a Fourth Amendment violation because no seizure occurred since he was not threatened with arrest and merely left the airport); SOLOVE & SCHWARTZ, supra note 88, at 726.

92. Sai Teja Peddinti et al., *User Anonymity on Twitter*, 15 SOCIOTECHNICAL SEC. & PRIVACY 84 (2017).

a. Open Fields Doctrine

The open fields doctrine means that there is no reasonable expectation of privacy in an individual's "open fields."[93] Typically in cases involving newer technology, courts have asked if the surveillance technology is one that is available to the public, and if it is, then the search falls under the open fields doctrine.[94] Twitter activity is particularly vulnerable to surveillance under the open fields doctrine because public profiles are constantly visible to the public.

However, while all tweets may be visible, the identity of a pseudonymous Twitter account will be unknown. Social media monitoring software, discussed in Part II.B, possibly constitutes technology unavailable to the public.[95] The combination of the pseudonymous handle in addition to the amount of information that can be obtained with surveillance software creates a likely actual expectation of privacy. Someone creating a pseudonymous account is doing with the expectation that the viewers will not know their identity. Additionally, much of the underlying information discovered by surveillance software is also thought of as private, such as location information or charting online relationships.[96]

It is likely that society would then recognize the expectation as reasonable because if there was no expectation of privacy, it is unlikely many people would create pseudonymous Twitter accounts in the first place. Some might argue that society shouldn't recognize the same reasonable expectation of privacy for non-citizens because of the interests in regulating national security or an immigrant's expectation to be surveilled[97] however, as discussed in Section I.B, non-citizens in the United States are protected by the Fourth Amendment.[98]

Finally, the posts are public and by posting to social media account in the first place, even with a pseudonym, the user has assumed a risk. Posting on a public platform, even with a pseudonym, does not create the same expectation of privacy as growing plants in the interior of one's home. In the end, the request

93. SOLOVE & SCHWARTZ, supra note 88, at 302.

94. Dow Chemical Co. v. United States, 476 U.S. 227, 238 (1986).

95. Bousquet, *supra* note 48*;* Kimberly McCullough, *Why Government Use of Social Media Monitoring Software Is a Direct Threat to Our Liberty and Privacy*, ACLU (May 6, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/why-government-use-social-media-monitoring [https://perma.cc/7L3C-BZ3S].

96. Bousquet, *supra* note 48.

97. *See* Raquel Aldana, *Of Katz and "Aliens": Privacy Expectations and the Immigration Raids*, 41 U.C. DAVIS L. REV. 1081, 1089 (2008) ("Like cars or certain 'heavily regulated' businesses, immigrants have become so regulated that any Katz expectation of privacy to occupy spaces in silence without detection becomes unreasonable.").

98. *See supra* Section I.B.

of a pseudonymous Twitter handle could be a search even when using the open fields doctrine.

b. Third Party Doctrine

Typically, the reasonable expectation of privacy test does not apply when an individual reveals information to a third-party because the individual has assumed the risk and cannot expect the shared information to remain private.[99] The court first considered the third party doctrine in *Smith v. Maryland* and held that there was no expectation of privacy in recorded phone numbers.[100] But, what is a third-party in this context and when is an individual voluntarily revealing information to a third-party such that the Fourth Amendment no longer protects the information?

An individual sharing information with third parties—that is, social media platforms, Internet Service Providers (ISPs), Online Service Providers (OSPs), and telephone companies—voluntarily reveals information if the individual knows the third-party could log the information or make records of the information.[101] This requirement focuses on the individual's knowledge that they are sharing information with a third party and that third party's technological ability to retain that information.[102] This is worrisome since many individuals share far more with third parties than they did in 1979 in *Smith v. Maryland*.[103] Individuals using social media share far more than phone numbers, such as GPS location data, acquaintance information, various thoughts in the form of status updates, personal photos, and political opinions. This creates privacy concerns that disproportionality harm immigrant and minority communities when the government collects social media handles from non-citizens.[104]

That location data does not fall under the third-party doctrine is evolving jurisprudence. In June 2018, the Supreme Court restricted the third-party doctrine in *Carpenter v. United States*[105] by holding that cell phone location information collected from third parties requires a warrant.[106] The Carpenter decision comes on the

99. Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine,* 130 HARV. L. REV. 1924, 1927–28 (2017).

100. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

101. *Id.* at 745; Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1048 (2008).

102. Oza, *supra* note 101, at 1048–49.

103. *Smith*, 442 U.S. at 735.

104. *See* Dawinder S. Sidhu, *The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim Americ*ans, U. MD. L.J. RACE RELIG. GENDER & CLASS 375, 392 (2007) (finding that post 9/11, many Muslim-Americans believed that U.S. government online surveillance was over inclusive and a small segment of Muslim-Americans changed their online behavior because of this belief).

105. 138 S. Ct. 2206 (2018).

106. *Id.* at 2223.

heels of *Riley v. California*,[107] which held that searching cell phones following an arrest requires a warrant.[108]

In *Carpenter*, Chief Justice Roberts first categorized cell phone location data as similar to the GPS data as the cell phone tracks every movement and can be used over a long period of time.[109] Individuals have a reasonable expectation that law enforcement will not track every single movement over a long period of time. Additionally, in *Carpenter*, Roberts distinguished the unique nature of cell phone location data to show why individuals have a reasonable expectation of privacy in that information.[110] For example, cell phones are pervasive, "a phone goes where its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[111]

Extending off the pervasive nature of cell phone use, Roberts in *Carpenter* stated that the traditional assumption of risk assumed in third-party doctrine cases was a fiction when applied to many new technologies.[112] Everyone has a cellphone and there's no affirmative action in sharing location with cell towers.[113] Additionally, Roberts argued that the cell phone location information reveals intimate details of a person's life.[114] Finally, the extraordinary amount of data, effortlessly compiled form cell phone data location tends to point away from a reasonable expectation of privacy.

While the court pointed out that *Carpenter* was a narrow holding limited to cell site location information, and not applicable to collection of other information involving national security,[115] similar themes appear in the information available by surveilling Twitter and other social media accounts. First, social media platforms contain and store information for long periods of time and even store location information. Like cellphones, Twitter use is pervasive. There are 321 million monthly active users on Twitter worldwide alone.[116] Furthermore, some of the data that users don't affirmatively share with ISPs the government may be able to access using social media monitoring software.[117] Finally, like the location data in Carpenter, the amount of data that can be collected

107. 573 U.S. 373 (2014).
108. *Id.* at 403.
109. *Carpenter*, 138 S. Ct. at 2218.
110. *Id.* at 2220.
111. *Id.* at 2217.
112. *Id.* at 2220.
113. *Id.*
114. *Id.*
115. *Id.*
116. *Number of Monthly Active Twitter Users in the United States from 1st Quarter 2010 to 4th Quarter 2018 (in millions)*, STATISTA, https://www.statista.com/statistics/274564/monthly-active-twitter-users-in-the-united-states/ [https://perma.cc/UY79-WLSA].
117. Bousquet, *supra* note 48.

effortlessly would seem to point away from a reasonable expectation of privacy.

Arguably, one voluntary assumes the risk of surveillance by posting publicly on Twitter. However, a pseudonymous account is less likely to be an assumption of risk since one has created an account not connected to oneself for a specific reason. Even more so than cell phone location information, Twitter accounts contain a portrait of a person's life: comments, arguments, ideas, thoughts, and expressions that one has shared for as long back as the account has been active. Additionally, all the accounts a user follows are also connected and the government may make inferences from these connections. What is more, Twitter accounts, even those anonymized, contain an extraordinary amount of data, including photos, thoughts, associations, speech, metadata, and location information.

When the account is pseudonymous, the user is assuming all of the account information is not connected to their identity and not assuming the risk of surveillance by immigration officials. By accessing pseudonymous accounts through just requesting social media handles, the immigration officials have effortlessly compiled far more information than they would have been able to in the past. This compilation of information from social media is similar to the mosaic theory introduced in *United States v. Jones*,[118] where Fourth Amendment protections might apply to the aggregation of GPS data over time.[119] Thus, the use of social media information in the form of Twitter handles to monitor immigrants implicates the mosaic theory and Fourth Amendment protections.

2. Is the Search Reasonable?

If indeed there was a search, which is possible, the next question is whether it is reasonable for immigration officers to collect Twitter handles. Typically, a search is considered reasonable if there is a warrant.[120] However, various exceptions apply. Such exceptions include search incident to arrest, consent searches, open fields, airport searches, and border searches.[121] The exception that the government is likely to invoke for the collection of social media handles is the "border search exception."[122] However, this exception

118. 565 U.S. 400 (2012).

119. *Id.* at 415–16 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . Awareness that the government may be watching chills associational and expressive freedoms.").

120. SOLOVE & SCHWARTZ, supra note 88, at 257.

121. Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473 (1985) (listing over twenty exceptions to both the warrant and probable cause requirement).

122. SOLOVE & SCHWARTZ, supra note 88, at 367.

only applies at the border or in various physical searches related to information seized at the border.[123] Additionally, if the government uses the social media handles to monitor immigrants once they are inside the United States, the border search exception likely doesn't apply because then it is no longer vetting.

B. *First Amendment: Anonymity and Chilling Effects*

The collection of Twitter handles by the government also implicates the First Amendment due to the speech involved. Additionally, chilling effects may still exist even if it does not amount to First Amendment protection. The First Amendment states "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble. . . ."[124] While laws directly forbidding certain types of speech are an obvious violation of the First Amendment, other laws that discourage certain types of speech may also subtly violate the First Amendment. This idea is known as a chilling effect, which was first referenced by the Supreme Court in *Wieman v. Updegraff*[125] as a "chill" upon freedom of thought and expression.[126] A governmental regulation that unjustly deters some sort of activity which is normally protected by the Constitution can also be a chilling effect.[127] With regard to monitoring of non-citizens via pseudonymous Twitter handles while they are in the United States, the First Amendment protects the rights to anonymity and the right to associate.[128]

Immigrants with pseudonymous Twitter accounts will likely experience a chilling effect from the collection of social media handles. The Supreme Court has consistently recognized the freedom of association and freedom to anonymous speech under the First Amendment.[129] It has also stressed the importance for individuals to freely associate and speak without the fear of

123. *Id.*
124. U.S. CONST. amend. I.
125. 344 U.S. 183 (1952).
126. *Id.* at 195.
127. *See* Frederick Shauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 B.U.L. REV. 685, 690 (1978).
128. This note recognizes that the same protections do not apply to non-citizens residing outside of the U.S. Zick, *supra* note 34, at 978 ("In sum, the few reported decisions and existing academic commentary seem generally to be in agreement that expressive guarantees do not apply extraterritorially to aliens."). However, the submission of social media handles is not limited to non-citizens outside of the U.S.
129. *See* Eric M. McLeod & Joseph S. Diedrich, *John Doe II and Political Speech: A Constitutional Perspective*, 90 WIS. LAW. 28, 31 (2017); *see also* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. Of Stratton, 536 U.S. 150, 166–66 (2002) (holding that ordinance requiring persons wishing to conduct door-to-door advocacy first obtain permits from the government violated First Amendment protections); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("[There is] a vital relationship between freedom to associate and privacy in one's associations.").

repercussions.[130] By denying these freedoms, the government would therefore create a chilling effect on speech and ability to associate with organizations and other affiliations.[131]

Twitter allows users to create pseudonymous accounts where the user may post opinions, engage in political discourse, and critique employers or other institutions without fear of repercussion by employers or family.[132] Additionally, the groups of other Twitter accounts that a pseudonymous Twitter user may follow or respond to frequently are likewise unaware of the identity of that user even though they may actively engage. The right to anonymity is protected under the First Amendment as way to present unpopular opinions without fear of prejudice and is celebrated as "a shield from the tyranny of the majority."[133]

The cases concerning the right to anonymity often involve the court holding regulations that require people to reveal their names to be unconstitutional.[134] When the government requires pseudonymous Twitter profiles from non-citizens, they are requesting access to information usually protected by the First Amendment.[135] While it may be debatable if the content under a pseudonymous account in a foreign country should be protected,[136] the content created while in the United States that can be monitored should be afforded greater protections.

Additionally, requiring immigrants to hand over Twitter handles, especially pseudonymous Twitter handles, threatens their

130. *See NAACP*, 357 U.S. at 460; *see also* Buckley v. Valeo, 424 U.S. 1, 25 (1976); Gibson v. Fla. Legis. Investigation Comm., 372 U.S. 539, 543 (1963).

131. *See* Shauer, *supra* note 127, at 690 (discussing how a chilling effect can be viewed as governmental regulation that unjustly deters some sort of activity which is normally protected by the Constitution).

132. An example of such an account is @BarristerSecret, or The Secret Barrister, a Twitter account held by an unnamed British barrister, or attorney. *See* @BarristerSecret, TWITTER (Mar. 6, 2019), https://twitter.com/BarristerSecret [https://perma.cc/CTF6-9N33]. This account and subsequent book candidly highlight the reality of the criminal justice system in the United Kingdom. SECRET BARRISTER, THE SECRET BARRISTER: STORIES OF THE LAW AND HOW IT'S BROKEN (2018). Indeed, in their blog post, The Secret Barrister states "anonymity buys me the ability to speak plainly, frankly and without fear or favour about the problems that I see in the criminal justice system, in a way that I don't think I could under my real name." *What's in a Name? Anonymity and Me*, SECRET BARRISTER (Mar. 22, 2018), https://thesecretbarrister.com/2018/03/22/whats-in-a-name-anonymity-and-me/ [https://perma.cc/SDK5-SSD7].

133. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (holding that an Ohio regulation requiring a signature on campaign pamphlets was impermissible because it made anonymity impossible and the right to decide to be anonymous was too important).

134. *See id.*

135. *See id.*

136. *See* Zick, *supra* note 34, at 975 ("Although alien speakers and audiences residing abroad can be substantially and directly affected by U.S. regulations and policies, the Supreme Court has never decided whether the First Amendment applies to any alien speech activity abroad. Courts and commentators, however, have generally been skeptical that aliens located abroad enjoy free speech protections.").

freedoms to speak and associate.[137] An immigrant living in the United States and in the process of seeking asylum from a government that targets dissenters may feel chilled knowing that the United States government now requires the collection of their pseudonymous Twitter account. Those seeking asylum for political dissent may be fearful if data in any database can connect their pseudonymous Twitter accounts with their actual identity. Immigrants may feel less able to share thoughts, ideas, and opinions fearing political or familial consequences or even fear for lives.

A pseudonymous Twitter user may also follow political, religious, and other organization pages that the government can make inferences from.[138] While *NAACP v. Alabam*a held that the government couldn't require the NAACP to hand over membership lists, the government here could collect associations through the individual rather than the organization. However, whether compelled disclosure of association comes to the organization or to the member, the constitution still protects the freedom of association.[139] The ability of CBP officers to look at accounts that a Twitter user follows and use Friend Mapper[140] to determine relationships and connections calls into question the right to freedom of association for immigrants and minority communities.

The government has a strong argument that the plenary power doctrine grants the executive power to regulate immigration in addition to protect the country in matters of national security.[141] Additionally, when it comes to standing, it is difficult to overcome the legal hurdle to establish a First Amendment violation based on a chilling effect in surveillance. In *Laird v. Tatum*,[142] the court

137. *See The Rights of Immigrants – ACLU Position Paper*, ACLU, https://www.aclu.org/other/rights-immigrants-aclu-position-paper [https://perma.cc/NQ5A-46TB] (stating that "once here, even undocumented immigrants have the right to freedom of speech and religion").

138. *See generally* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (arguing that GPS information can yield information detailing "familial, political, professional, religious, and sexual associations" and that the courts should "ask whether people reasonably expect that their [actions] will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will," such information).

139. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460 (1958) ("It 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.").

140. *See* WAGNER, *supra* note 46.

141. *See* U.S. CONST. art. II, § 3; United States *ex rel.* Knauff v. Shaughnessy, 338 U.S. 537, 543 (1950) ("Thus the decision to admit or to exclude an alien may be lawfully placed with the President, who may in turn delegate the carrying out of this function to a responsible executive officer of the sovereign, such as the Attorney General. The action of the executive officer under such authority is final and conclusive.").

142. *See* Laird v. Tatum, 408 U.S. 1, 15–16 (1972); John R. Vile, *Laird v. Tatum (1972)*, FIRST AMEND. ENCYCLOPEDIA, https://mtsu.edu/first-amendment/article/342/laird-v-tatum [https://perma.cc/C72Z-V7BN].

dismissed a challenge to a surveillance program that observed and collected information on known individuals because the chilling-effect harms were too speculative.[143] Under a *Laird* analysis, social media surveillance faces a difficult challenge because the harm will likely not be cognizable, and the government has a strong interest in monitoring non-citizens.[144]

CONCLUSION

While the disclosure of social media handles may seem as innocuous as revealing one's name or email address, the policy reasoning and past government surveillance practices hint at greater privacy concerns. The vast amount of information available on social media makes the collection and future monitoring of those accounts suspect. While under current precedent the Fourth and First Amendment provide few protections for immigrants, courts have slowly begun to recognize the problems new technology poses for constitutional rights. *Carpenter* acknowledged "the exhaustive chronicle of location information casually collected by wireless carriers today."[145] Additionally, the dissent in *Fifth Avenue Peace Parade Committee v. Gray*[146] identified the trend of taking away constitutional rights, such as the right to associate, "on the basis of national security."[147] The overt collection and use of social media handles to regularly monitor immigrants in the United States and the few protections provided by the First and Fourth Amendment show how little protections may exist in the monitoring of even pseudonymous social media accounts in a broader context.

143. 408 U.S. 1 (1972).

144. *See id.* at 13–14 (finding that a showing of "specific present objective harm or a threat of specific future harm" is necessary for standing); Gayle Horn, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines*, 60 N.Y.U ANN. SURV. AM. L 735, 753–54 (2005); *see also* Eric Lardiere, *The Justiciability and Constitutionality of Political Intelligence Gathering*, 30 UCLA L. REV. 976, 1006–07 (1983).

145. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

146. 480 F.2d 326 (2d Cir. 1973).

147. *Id.* at 333 (Oakes, J., dissenting).