Watching and Waiting: Modern Social Media Surveillance of Immigrants and Fourth Amendment Implications

Vaishali Nambiar*

TABLE OF CONTENTS

* J.D., May 2025, The George Washington University Law School; B.A. 2021 Community and Global Public Health, University of Michigan. I am deeply grateful to the late Professor Ethan Lucarelli, whose thoughtful guidance was instrumental in the development of this Note. I also extend my sincere thanks to the FCLJ Editorial Board for their dedication throughout this process. A special acknowledgment goes to Professor Daniel Solove for sparking my passion for privacy law and for his invaluable mentorship. Finally, to my parents—there are no words that could ever fully convey my appreciation for your unconditional love and support.

I. INTRODUCTION

The Internet is ubiquitous—permeating our commerce, culture, and daily life.[1] Over the last decade, technological developments have created an online world that feels like a natural extension of the physical world. Social media platforms are a major force in the online world. These platforms create an environment for online users to interact with each other, typically by way of engaging with user-generated content or private messaging features.[2] Today, there are approximately 4.9 billion social media users worldwide, and the average user now spreads their digital footprint across six to seven different platforms.[3] Essentially, social media platforms have become hubs for the massive accumulation of valuable personal data. One consequence of this is that the government often engages in surveilling social media users and collecting and analyzing their personal data; and immigrants are among the communities most significantly impacted by this issue because they tend to face increased scrutiny by law enforcement.[4]

There are various approaches to social media surveillance, and there is evidence that the government is increasingly moving towards utilizing machine learning technology and automated tools to collect and analyze social media data.[5] These tools are powerful because they make many aspects of surveillance much more efficient, allowing for quick data aggregation and analysis.[6] For example, in 2018, law enforcement was able to locate and arrest an immigrant using the pseudonym "Sid," solely by way of photos and status updates he posted on Facebook.[7] This tracking was conducted by data mining firms U.S. Immigration and Customs Enforcement ("ICE") contracted with at the time, and ultimately, Sid was "only one of thousands of individuals" ICE was tracking at that point.[8]

This Note will argue that courts are currently not reading the Fourth Amendment broadly enough to afford adequate privacy protections to immigrants against social media surveillance carried out by law enforcement.

---

1. *See* Jacob Poushter, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, PEW RSCH. CTR. (Feb. 22, 2016), https://www.pewresearch.org/global/2016/02/22/internet-access-growing-worldwide-but-remains-higher-in-advanced-economies/ [https://perma.cc/KUT2-SBHX].

2. *See* Ben Lutkevich, *What is Social Media?*, TECHTARGET, https://www.techtarget.com/whatis/definition/social-media [https://perma.cc/5FWB-6PAB] (last visited Nov. 5, 2024).

3. *See* Belle Wong, *Top Social Media Statistics and Trends of 2024*, FORBES ADVISOR (May 18, 2023, 2:09 PM), https://www.forbes.com/advisor/business/social-media-statistics/ [https://perma.cc/R4LY-W3MV].

4. *See* Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, BROOKINGS (Apr. 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/5MLB-ENSH].

5. *See* Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FOUND. (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance/ [https://perma.cc/MP7L-XW3X].

6. *See* Lee & Chin-Rothmann, *supra* note 4.

7. *See id.*

8. *Id.*

Due to the evolving nature of user expectations of privacy online and the expansive nature of modern surveillance techniques utilized by law enforcement, this Note argues that courts should adopt a more expansive view of the Fourth Amendment's protections to ensure individual privacy is protected in an increasingly digital world. This Note addresses the major contexts in which law enforcement conducts social media surveillance on immigrants: searches at the border and during visa processing.

Section I will discuss how, historically, immigrant surveillance in the United States has consistently iterated and adapted to the latest technologies of the time. This section also details the role political administrations and key federal agencies, like the U.S. Customs and Border Protection ("CBP") and ICE, have played in implementing specific surveillance initiatives over the last decade. Section II will outline major court cases that have shaped how courts understand the Fourth Amendment to protect individual privacy interests relative to governmental interests in surveillance. More specifically, this section will detail the various legal tests and doctrines, such as the reasonable expectation of privacy test and the third-party doctrine, that help courts determine whether an individual has a cognizable privacy interest. Subsequently, the Analysis section will advance the argument that immigrants maintain a reasonable expectation of privacy in their social media data and that courts should read the Fourth Amendment to recognize this privacy interest, particularly after the Supreme Court's decision in *Carpenter*. In the final section, this Note will propose legal and policy recommendations to provide more adequate protection for the privacy interests of immigrant populations.

II. BACKGROUND

A. The State of Immigrant Surveillance in the United States

This part of the Note will provide an overview of the state of immigrant surveillance in the United States. The first section will discuss methods law enforcement has historically utilized for surveillance, as well as detail the role of the Department of Homeland Security in implementing immigrant surveillance programs. Next, this Note will describe the rise of social media platforms over the last decade, and how this trend led to the creation of several surveillance initiatives during former President Trump's presidency that centered on social media data. Finally, the third section will categorize the different approaches that law enforcement agencies have taken with respect to modern social media surveillance.

1. The U.S. Immigration System & Historical Approaches to Surveillance

Immigrant populations in the United States have historically been targets of excessive government surveillance.[9] Modern approaches to the monitoring of immigrant populations can be traced back to the methods adopted by police in the 19th century to target areas of cities where high concentrations of immigrants resided.[10] In the 19th century, law enforcement utilized the new technologies of the time for surveillance, like fingerprinting, and adopted excessive data retention practices, by collecting and storing masses of files containing profiles of immigrants.[11] These surveillance approaches have only grown more powerful with technological advancements in recent years.[12] More specifically, law enforcement today leverages machine learning and AI-powered technology as part of its surveillance agenda to both collect information and enable seamless data retention and information sharing between law enforcement agencies.[13]

Today, several federal agencies handle immigration and immigrant surveillance.[14] The focus of this Note will be on the surveillance practices of the Department of Homeland Security ("DHS") and the State Department. DHS houses 16 different offices, but the two most relevant to immigrant surveillance are CBP and ICE.[15] While CBP is responsible for securing the border, ICE enforces immigration laws in non-border areas and handles detention and deportation.[16] The Department of State houses several smaller bureaus and offices, but the Bureau of Consular Affairs ("BCA") is one of the most dominant agencies in the context of immigrant surveillance, as it is the office primarily responsible for issuing United States visas and adjudicating visa applications of aliens outside the country.[17] Another important element of this structure is the Privacy and Civil Liberties Oversight Board ("PCLOB"). PCLOB is an independent agency that provides oversight to ensure there is a balance between the federal government's anti-terrorism

9. *See* Matthew Guariglia, *How the Surveillance of Immigrants Remade American Policing*, TIME (Nov. 21, 2023, 2:32 PM), https://time.com/6336882/police-surveillance-history/ [https://perma.cc/KE7A-2FRH].

10. *See id.*

11. *See id.*

12. *See generally* Faiza Patel et al., *Social Media Monitoring*, BRENNAN CTR. FOR JUST. (Mar. 11, 2020), https://www.brennancenter.org/our-work/research-reports/social-media-monitoring [https://perma.cc/G763-CJJJ].

13. *See id.*

14. *See generally* Megan Davy et al., *Who Does What in U.S. Immigration*, MIGRATION POL'Y INST. (Dec. 1, 2005), https://www.migrationpolicy.org/article/who-does-what-us-immigration [https://perma.cc/3K4T-T35Z].

15. *See Operational and Support Components*, U.S. DEP'T HOMELAND SEC., https://www.dhs.gov/operational-and-support-components [https://perma.cc/4ZPJ-8EHG] (last visited Jan. 24, 2024).

16. *See* Davy et al., *supra* note 14.

17. *See id.*; *see also Bureaus of Consular Affairs*, U.S. DEP'T OF STATE, https://www.state.gov/bureaus-offices/under-secretary-for-management/bureau-of-consular-affairs/ [https://perma.cc/LUV6-EFHD] (last visited Jan. 24, 2024).

efforts and the interests of privacy and civil liberties.[18] In 2007, Congress passed Section 803 of the Implementing Recommendations of the 9/11 Commission Act, which required eight federal law enforcement agencies—including DHS and the State Department—to issue reports to Congress and PCLOB about their work.[19] The Board regularly publishes publicly available reports detailing their activities and recommendations for various federal government surveillance issues.[20]

Though federal law enforcement agencies are responsible for the implementation of surveillance programs, over the years, political and social factors have also played a dominant role in shaping public sentiment toward immigrants and in influencing attitudes toward the monitoring of immigrant communities.[21] One of the most significant examples is the 2001 USA PATRIOT Act, which was bipartisan legislation passed after the 9/11 terrorist attacks to grant law enforcement agencies greater surveillance powers and to ease the process by which agencies could collect foreign intelligence information.[22] Another major topic defining anti-migrant rhetoric in recent years is the U.S.-Mexico border crisis.[23] The U.S.-Mexico border has been described as one of the "most politicized spaces in the country," likely in part due to invasive surveillance by law enforcement in this area.[24] Surveillance tactics employed in this area over the years include cell phone searches at the border, facial recognition technology, real-time crime analytics, and the use of drones and mobile surveillance vehicles.[25]

---

18. *See History and Mission*, U.S. PRIV. & CIV. LIBERTIES OVERSIGHT BD., https://www.pclob.gov/About/HistoryMission [https://perma.cc/8ZBR-6W4P] (last visited Jan. 24, 2024).

19. *See id.*

20. *See id.*

21. *See* Besheer Mohamed, *Muslims are a Growing Presence in U.S., but Still Face Negative Views From the Public*, PEW RSCH. CTR. (Sept. 1, 2021), https://www.pewresearch.org/short-reads/2021/09/01/muslims-are-a-growing-presence-in-u-s-but-still-face-negative-views-from-the-public/ [https://perma.cc/5V9C-MHQH] (discussing public attention on Muslim Americans after 9/11 and how Americans' view of Muslims has become increasingly polarized along political lines).

22. The key statute regulating foreign intelligence gathering within the United States is the Foreign Intelligence Surveillance Act of 1978. The Act was designed as a permissive law to allow the government to engage in foreign intelligence gathering. Under the 1978 law, law enforcement had to show the "primary purpose" of their investigation was foreign intelligence. However, after the PATRIOT Act was passed, the bar was lowered to be "significant purpose." *See Surveillance Under the USA/Patriot Act*, AM. C.L. UNION (Oct. 23, 2001), https://www.aclu.org/documents/surveillance-under-usapatriot-act [https://perma.cc/7TPC-WUTA]; *see generally EFF Analysis of the Provisions of the Provisions of the USA PATRIOT Act*, ELEC. FRONTIER FOUND. (Oct. 27, 2003), https://www.eff.org/deeplinks/2003/10/eff-analysis-provisions-usa-patriot-act [https://perma.cc/998A-A6ZW].

23. *See* Saira Hussain, *Surveillance and the U.S.-Mexico Border: 2023 Year in Review*, ELEC. FRONTIER FOUND. (Dec. 21, 2023), https://www.eff.org/deeplinks/2023/12/surveillance-and-us-mexico-border-2023-year-review [https://perma.cc/5J9M-FWUS]; *see also* Dana Khabbaz, *How CBP Uses Hacking Technology to Search International Travelers' Phones*, EPIC (Feb. 22, 2022), https://epic.org/how-cbp-uses-hacking-technology-to-search-international-travelers-phones/ [https://perma.cc/DL84-JQQ5].

24. Hussain, *supra* note 23.

25. *See id.*

2. The Rise of Social Media Surveillance

As discussed in the Introduction, there are almost 5 billion social media users worldwide. Social media companies have become a mainstay in people's lives, perhaps because they have continued to expand beyond their original use of giving users a public forum for interaction.[26] For example, platforms like X (formerly Twitter) or Reddit fall under the label of "social media" but are often used by individuals as a means for passive news gathering rather than public interaction.[27] Another example is TikTok, where many individuals create accounts solely as a means for consuming entertaining content that the algorithm feeds them rather than engaging with people they know in their real lives.[28] Ultimately, as social media continues to sustain the attention of individuals, more valuable personal data accumulates on these platforms—evidenced by the rise of targeted advertisers on social media platforms hoping to capitalize.[29]

There have been several efforts over the years to capitalize on the valuable data available on social media and implement social media monitoring programs, particularly during the Trump administration.[30] Former President Donald Trump's presidency was marked by anti-migration policies targeting persons entering through the U.S.-Mexico border and initiatives like "The Muslim Ban" that received widespread criticism from immigrant rights activists.[31] With respect to monitoring specifically, President Trump actively endorsed several new immigrant surveillance efforts by agencies like DHS and the State Department between 2017–2019.[32] For example, as part of the "Muslim Ban" executive orders, the State Department issued an emergency notice in May 2017 to increase screening and information collection by requiring visa applicants to provide a list of social media identifiers they had used within the previous 5 years.[33]

A critical turning point in law enforcement's approach to social media surveillance came in July 2017 when ICE announced it was searching for data-mining firms to implement a monitoring program driven by automated

---

26. Katie Fleeman, *Social Media and Reader Engagement*, KNIGHT SCI. JOURNALISM, https://ksjhandbook.org/social-media-reader-engagement/different-platforms-different-audiences/ [https://perma.cc/9HLE-RUS4] (last visited Mar. 3, 2024).

27. *Id.*

28. *See* Mostafa ElBermawy, *Social Media is Dead: From Connection to Consumption*, NOGOOD (July 27, 2022), https://nogood.io/2022/07/27/social-media-is-dead/ [https://perma.cc/U492-UGQG].

29. *See* Nik Froehlich, *The Truth in User Privacy and Targeted Ads*, FORBES (Feb. 25, 2022, 9:29 AM), https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/?sh=6c40c8bc355e [https://perma.cc/X9VJ-9PCV].

30. *See Social Media Surveillance*, ASIAN AMS. ADVANCING JUST. 1 (Feb. 11, 2020), https://www.advancingjustice-aajc.org/sites/default/files/2020-02/Social%20Media%20Surveillance%20Backgrounder.pdf [https://perma.cc/X827-AWU5].

31. Adam Isacson et al., *Putting the U.S.-Mexico 'Border Crisis' Narrative into Context*, WASH. OFF. ON LAT. AM. (Mar. 17, 2021), https://www.wola.org/analysis/putting-border-crisis-narrative-into-context-2021/ [https://perma.cc/5P53-VV6H].

32. *See Social Media Surveillance*, *supra* note 30.

33. *See id.*

technology. [34] The "Extreme Vetting Initiative Program" proposed to constantly monitor social media posts by U.S. visitors and "streamline the current manual vetting process while simultaneously making determinations via automation if the data retrieved is actionable."[35] However, after receiving strong public pushback, ICE withdrew the proposal and rebranded the program as the "Visa Lifecycle Vetting Initiative" ("VLVI").[36] Through the VLVI, in June 2018, ICE spent $100 million to hire 180 people to continuously monitor 10,000 foreign visitors flagged as high-risk.[37]

Despite the seeming shift back to a human-driven decision-making process, concerns still remain. In February 2018, President Trump announced the establishment of a "National Vetting Enterprise" ("NVE") within the DHS' National Vetting Center ("NVC").[38] NVC's stated mission is to streamline intelligence information sharing between agencies to "ensure that immigration and border security decisions are fully informed and accurately implemented."[39] Some critics note that the establishment of the NVE, taken along with DHS rhetoric and directives, seems to suggest a "persistent interest in incorporating machine learning technology in the future in immigration vetting functions."[40]

This is a troubling issue because several machine learning-driven tools employed by DHS are not capable of accurately analyzing users posts.[41] For example, "algorithmic tone and sentiment" analytics, which try to uncover user sentiments and beliefs from their posts, were only found to make accurate predictions of users' political ideologies on Twitter 27% of the time.[42] The problem only compounds when tools analyze user posts that are in different languages and nonstandard dialects.[43]

A separate issue with these initiatives is that many of them have been rolled out as pilot programs.[44] As a result, there is little publicly released

---

34. *See* Sam Biddle & Spencer Woodman, *These are the Technology Firms Lining Up to Build Trump's "Extreme Vetting" Program*, INTERCEPT (Aug. 7, 2017, 1:45 PM), https://theintercept.com/2017/08/07/these-are-the-technology-firms-lining-up-to-build-trumps-extreme-vetting-program/ [https://perma.cc/T29S-6B4V].

35. *See id.*; *see also* George Joseph & Kenneth Lipp, *How ICE is Using Big Data to Carry Out Trump's Anti-Immigrant Crusade*, SPLINTER NEWS (Aug. 11, 2017, 6:30 PM), https://splinternews.com/how-ice-is-using-big-data-to-carry-out-trumps-anti-immi-1797745578 [https://perma.cc/4GQF-37BC].

36. Patel et al., *supra* note 12.

37. *See id.*

38. Chinmayi Sharma, *The National Vetting Enterprise: Artificial Intelligence and Immigration Enforcement*, LAWFARE (Jan. 8, 2019, 9:00 AM), https://www.lawfaremedia.org/article/national-vetting-enterprise-artificial-intelligence-and-immigration-enforcement [https://perma.cc/E5KB-PTYP].

39. *National Vetting Center FAQs*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/border-security/ports-entry/national-vetting-center [https://perma.cc/JQ9K-UY8M] (last visited Jan. 24, 2024).

40. Sharma, *supra* note 38.

41. *See* Patel et al., *supra* note 12.

42. *Id.*

43. *See id.*

44. Patel et al., *supra* note 12, at 26.

information about program implementation or success.[45] The most recent guidance discussing these measures seems to be a 2016 report from the DHS Office of the Inspector General ("OIG") about ICE's use of social media monitoring during the visa issuance process. In that report, the DHS OIG found that ICE pilot programs, including those involving automated searches, lacked adequate metrics for measuring efficacy.[46] Further, the report recommended that USCIS and ICE create a plan with more "well-defined, clear, and measurable objectives and standards for determining pilot performance."[47] With respect to other surveillance programs, recent documents obtained by the Knight First Amendment Institute from the Office of the Director of National Intelligence ("ODNI"), the head agency overseeing the U.S. intelligence community, reveal ODNI staff acknowledging that the collection of social media identifiers are "useless" to the immigration screening process.[48]

3. Categories of Social Media Surveillance

Aside from pilot programs, there are three common methods of social media monitoring that law enforcement agencies utilize. First, government agencies often purchase data from private surveillance companies.[49] Government agencies like ICE and CBP have a history of contracting with data mining firms for assistance in collecting and analyzing social media data.[50] For example, CBP contracted with data mining firm Palantir to design a framework that identified non-obvious links between individuals based on a variety of information, including social media data.[51] Another example is ICE's partnership with data mining firm, Giant Oak, for support on a surveillance program implementing continuous monitoring for immigrants under the agency's visa applicant screening program.[52] Through the partnership, Giant Oak supplied ICE with the "Giant Oak Search Technology

45. *See id.*

46. *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success*, U.S. DEP'T HOMELAND SEC. (Feb. 27, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf [https://perma.cc/MSS3-ZULT] [hereinafter *DHS Social Media Screening*].

47. *Id.*

48. *See State Department Rule Requiring Visa Applicants to Register Their Social Media Handles is Ineffective New Documents Say*, KNIGHT FIRST AMEND. INST. (Oct. 5, 2023), https://knightcolumbia.org/content/state-department-rule-requiring-visa-applicants-to-register-their-social-media-handles-is-ineffective-new-documents-say [https://perma.cc/W7Z5-CUC7] [hereinafter *State Department Rule Ineffective*].

49. *See Social Media Surveillance*, *supra* note 30; *see* Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELEC. FRONTIER FOUND. (Dec. 2, 2019), https://www.eff.org/wp/behind-the-one-way-mirror#Data-brokers [https://perma.cc/4WWG-2TAW] (explaining that "data broker" is a broad term, but it often refers to firms that purchase and assemble data from a variety of smaller companies and streams to eventually sell).

50. *See Social Media Surveillance*, *supra* note 30.

51. *See id.*

52. *See id.*

System" ("GOST").[53] GOST provides "behavioral-based [I]nternet search capabilities," enabling analysts to review an individual's social media profile, provide a social graph of their connections, and assigns them a rating—"thumbs up" or "thumbs down."[54]

Another approach to monitoring is the government's collection of social media data through visa applications, like the DS-160 and DS-260.[55] Before Trump took office in January 2017, DHS had already started implementing a process of requesting foreign travelers arriving through the Visa Waiver Program to voluntarily provide their social media handles.[56] These forms request visa applicants to voluntarily provide their social media usernames for any social media accounts they have owned in the preceding 5 years.[57] The information applicants provide on these applications is compared against other DHS databases, and a copy of their application is stored in CBP's Automated Targeting System ("ATS").[58]

The third category of social media monitoring is through searches occurring at the border. Here, typically, ICE extracts social media data from electronic devices during the course of a border search.[59] Afterward, ICE may use its analytical tool, the FALCON Search & Analysis System ("FALCON-SA"), to analyze the collected social media data and generate reports to inform agency decision-making and strategy.[60] Some of the tool's analytical capabilities include presenting relationships between different entities and people, graphical depictions of the chronology in which events occurred, and geospatial placement of entities or events on a map.[61] Particularly concerning is the fact that once extracted and analyzed, the collected data can also be stored and shared across other law enforcement agencies.[62]

---

53. Joseph Cox, *Inside ICE's Database for Finding "Derogatory" Online Speech*, 404 MEDIA (Oct. 24, 2023, 9:00 AM), https://www.404media.co/inside-ices-database-derogatory-information-giant-oak-gost/ [https://perma.cc/4LQ2-5P6M].

54. *Id.* (quoting a GOST user guide).

55. *See Social Media Surveillance*, *supra* note 30.

56. *See id.* (the Visa Waiver Program is a program allowing "citizens of 38 countries to travel and stay up to 90 days without a visa").

57. *See id.*

58. *See* DHS/U.S. Customs and Border Protection (CBP)–009 Electronic System for Travel Authorization (ESTA) System of Records, 81 Fed. Reg. 39680, 39681 (June 17, 2016); *see also* U.S. DEP'T HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM at 94 (2017) https://www.dhs.gov/sites/default/files/2022-07/privacy-pia-cbp006-ats-july2022_0.pdf [https://perma.cc/VC39-EGPA] ("ATS compares information about individuals entering and exiting the country . . . with other identified patterns requiring additional scrutiny based on CBP Officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence.").

59. *See* Patel et al., *supra* note 12, at 28.

60. *See id.*

61. *See* Jonathan R. Cantor, *Privacy Impact Assessment Update for the FALCON Search and Analysis System*, U.S. DEP'T HOMELAND SEC. (Oct. 11, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice032b-falconsa-appendixbupdate-march2021.pdf [https://perma.cc/7XDF-AU4B].

62. *See* Patel et al., *supra* note 12, at 28.

B. Fourth Amendment Framework

This section will provide the legal framework for how the Fourth Amendment's protections are interpreted. For the Fourth Amendment to apply, the court must find that a "search" or "seizure" has occurred.[63] Under the Supreme Court's Fourth Amendment jurisprudence, a search exists where an individual has a "reasonable expectation of privacy"—an actual or subjective expectation of privacy that society is prepared to recognize as reasonable.[64] However, the Supreme Court has found an expectation of privacy is not reasonable when individuals voluntarily provide their information to third parties, like businesses and institutions.[65] Additionally, the Supreme Court has found in multiple cases that routine searches and seizures by law enforcement at the border do not offend the Fourth Amendment.[66] Applying this framework to the modern context of digital search has presented challenges, as lower courts have had to grapple with how much they are willing to recognize digital norms and expand collective notions of the "reasonable expectation of privacy."[67]

1. Reasonable Expectation of Privacy Test

The Fourth Amendment protects people from unreasonable searches and seizures by the government.[68] Moreover, any "searches deemed necessary should be as limited as possible."[69]

To determine whether there has been a search or seizure to which the Fourth Amendment applies, courts apply the "reasonable expectation of privacy test," which originates from *Katz v. United States*.[70] In *Katz*, the FBI wiretapped the outer part of a public phone booth to record the defendant's phone conversation and the prosecution attempted to enter these recordings into evidence.[71] In a landmark decision, the Supreme Court reversed the trial and appellate courts' decision to admit the recordings because it found that Katz was justified in believing that his phone conversation would remain private, though it took place in a public phone booth.[72] As noted in Justice Harlan's concurrence in *Katz*, the Court arrived at this conclusion by applying the reasonable expectation of privacy test, which asks whether a person has an actual or subjective expectation of privacy and if this expectation of privacy is one that society is prepared to recognize as reasonable.[73] If the answer to both parts is yes, then the Fourth Amendment applies.[74] Before *Katz*, Courts took a property-based approach (commonly referred to as the

63. U.S. Const. amend. IV (protecting "against unreasonable searches and seizures").
64. *See* discussion *infra* Section I.B.1.
65. *See* discussion *infra* Section I.B.2.
66. *See* discussion *infra* Section I.B.3.
67. *See* discussion *infra* Section I.B.4.
68. *See* U.S. CONST. amend. IV.
69. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).
70. *See* Katz v. United States, 389 U.S. 360, 516 (1967).
71. *See id.* at 348.
72. *See id.* at 352–53.
73. *See id.* at 516 (Harlan, J., concurring).
74. *See id.*

"physical trespass doctrine") that only recognized Fourth Amendment violations where there was a physical intrusion on one's property.[75] However, the *Katz* case marked an expansion in the Court's understanding of Fourth Amendment violations—with the Court famously writing that "the Fourth Amendment protects *people*, not places."[76]

Nonetheless, in *U.S. v. Jones*, the Supreme Court clarified that *Katz* did not replace the physical trespass doctrine with the reasonable expectation of privacy test, but rather it added to it.[77] In *Jones*, the FBI placed a GPS tracker on a defendant-suspect's vehicle to continuously track his movements for a month.[78] The government argued that the defendant could not have a reasonable expectation of privacy in his movements through public streets.[79] However, the Court rejected this argument, noting that *Katz* aside, the placement of the tracker on the vehicle was a *physical trespass* that constituted a search within the scope of the Fourth Amendment under the physical trespass doctrine.[80] The Court further reiterated that under *Katz* individuals may still retain a reasonable expectation of privacy over things that happen in public.[81]

2. The Third-Party Doctrine

In *Smith v. Maryland*, the Supreme Court created the third-party doctrine, which essentially states that people do not have a reasonable expectation of privacy in the things they voluntarily entrust to third parties.[82] In *Smith*, the police requested a telephone company to record the numbers the defendant, Smith, was dialing and used the collected evidence to charge him with a crime.[83] Smith tried to suppress the evidence on the basis of the Fourth Amendment, arguing that he had a reasonable expectation of privacy for conversations in his home and that the police did not obtain a warrant to conduct this search.[84] Ultimately, the Court held that Smith did not have a reasonable expectation of privacy in the numbers he dialed—because he should have known his phone company had a record of this information.[85] The Court justified the third-party doctrine by citing to a string of other cases applying a similar legal framework (now commonly referred to as the "misplaced trust doctrine").[86]The misplaced trust doctrine essentially provides that when someone voluntarily divulges information to another, they

75. *See generally* Olmstead v. United States, 277 U.S. 438 (1928).
76. *See Katz*, 389 U.S. at 351.
77. *See* United States v. Jones, 565 U.S. 400, 409 (2012).
78. *See id.* at 402–03.
79. *See id.* at 406.
80. *See id.* at 404–07.
81. *See id.* at 406–07.
82. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
83. *See id.* at 737.
84. *See id.*
85. *See id.* at 742–43.
86. *Id.* at 743–44.; *see* Allyson W. Haynes, *Virtual Blinds: Finding Online Privacy In Offline Precedents*, 14 VAND. J. ENT. & TECH. L. 603, 623 (2012).

assume the risk of betrayal.[87] This is typically applied in situations where law enforcement goes undercover to deceive someone for the purposes of information gathering.[88] However, as the dissent in *Smith* notes, a crucial distinction between the two doctrines is that in the undercover agent scenario, the defendant typically exercises more voluntary discretion in revealing personal details.[89] In contrast, in situations arising under the third-party doctrine, the defendant must be willing to avoid using technology that has become a "personal or professional necessity" in order to avoid surveillance.[90]

Since *Smith* was decided in 1979, the third-party doctrine has persisted and created a channel for law enforcement to directly compel data from companies without a search warrant.[91] As a result, some social media companies, like Meta, have dedicated sections on their websites with various metrics regarding the number and types of information requests they receive from law enforcement over a specific period.[92] Additionally, the company may detail its policy for handling these requests.[93] For example, Meta's page provides that the volume of requests it receives has increased steadily—from approximately 37,000 in 2015 to 147,000 in 2023.[94] Moreover, between January and June 2023, law enforcement made 13,511 requests by way of a subpoena, implicating a total of 28,700 users/accounts.[95] Meta addressed and produced some data for 83% of these requests.[96]

Nonetheless, the third-party doctrine has faced a great deal of criticism in recent years, particularly in an age where so much personal data exists online in the hands of third parties.[97] In fact, courts have been moving towards narrowing the scope of the third-party doctrine.[98] Most significant in recent years was the Supreme Court's 2018 decision in *Carpenter v. United States*. In this case, the government suspected the defendant of a series of robberies, so they requested the defendant's wireless carriers to provide his cell-site location information ("CSLI") records to verify where he was when the

87. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966).

88. *See generally id.*; On Lee v. United States, 343 U.S. 747 (1952)*;* United States v. White, 401 U.S. 745 (1971).

89. *See Smith*, 442 U.S. at 749–50.

90. *Id.* at 750.

91. *See* Brent Skorup, *Tech Companies' Terms of Service Agreements Could Bring New Vitality to the Fourth Amendment*, HARV. L. REV. (Sept. 9, 2024), https://harvardlawreview.org/blog/2024/09/strongtech-companies-terms-of-service-agreements-could-bring-new-vitality-to-the-fourth-amendment-strong/ [https://perma.cc/YD54-TTXD].

92. *See Government Request for User Data*, META, https://transparency.fb.com/reports/government-data-requests/country/US/ [https://perma.cc/XUF5-8JSZ] (last visited Nov. 7, 2024).

93. *See id.*

94. *See id.*

95. *See id.*

96. *See id.*

97. *See* Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After Carpenter*, 26 B.U. J. SCI. & TECH. L. 286, 297 (2020) (describing the third-party doctrine as "one of the most critiqued aspect(s) of Fourth Amendment jurisprudence").

98. *See* United States v. Warshak, 631 F.3d 266, 284-286 (2010) (holding that the government could not compel a commercial ISP to turn over the content of their subscriber's emails without a warrant, and noting the Fourth Amendment should keep up with modern technology).

robberies occurred.[99] The carriers complied with the request and provided the police with records indicating all of the cell-sites Carpenter's phone used over the course of four months.[100] It may seem third-party doctrine would apply here, but the Supreme Court held that there was a reasonable expectation of privacy in extensive records of historical CSLI held by third parties.[101]

Though the Court did not completely eliminate the third-party doctrine in *Carpenter*, it narrowed it by recognizing the amount of data at issue was so vast and revealing.[102] In his dissenting opinion, Justice Kennedy pointed to six specific factors and considerations that influenced the Supreme Court's decision that the third-party doctrine did not apply to the surveillance of CSLI data. These factors were: (1) how revealing the data was, (2) the amount of data collected, (3) the number of people affected, (4) the inescapable nature of the surveillance, (5) whether the disclosure of data to the third party is automated, and (6) the difficulty of conducting surveillance.[103] Despite these factors being enumerated most clearly in a dissenting opinion, some legal scholars have coined these the "*Carpenter* factors" and used the factors to interpret the decision.[104]

3. The Border-Search Exception

One major exception to the scope of the Fourth Amendment's protections is border searches, which means that law enforcement may conduct routine searches and seizures at the border without probable cause or a warrant.[105] This exception is often justified by a need to balance Fourth Amendment interests and the right to privacy against legitimate governmental interests, like national security.[106]

The border search exception is relevant to social media monitoring because a key method law enforcement uses to collect social media information from immigrants is through searches of smartphones and digital devices at the border. In 2022, CBP conducted approximately 45,499 border searches of electronic devices.[107] While federal courts have consistently applied the exception in circumstances involving a physical search at the border, in recent years, some courts have been more hesitant to apply the exception in cases of searching digital data.[108]

---

99. *See* Carpenter v. United States, 585 U.S. 296, 301–03 (2018).

100. *See id.*

101. *See id.* at 309.

102. *See id.* at 311–12.

103. *See id.* at 339–40.

104. *See, e.g.*, Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of the Fourth Amendment*, 135 HARV. L. REV. 1790, 1800 (2022).

105. *See* United States v. Ramsey, 431 U.S. 606, 616–17 (1972).

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

107. *See* Sophia Cope, *Federal Judge Makes History in Holding that Border Searches of Cell Phones Require a Warrant*, ELEC. FRONTIER FOUND. (May 30, 2023), https://www.eff.org/deeplinks/2023/05/federal-judge-makes-history-holding-border-searches-cell-phones-require-warrant [https://perma.cc/TZ2B-QAMT].

108. *See id.*

One reason for this trend is likely the Supreme Court's 2014 decision in *Riley v. California*. In *Riley*, the police searched the defendant during an arrest and seized his cell phone.[109] After conducting a search of the phone, the police subsequently introduced items found during the search into evidence during trial.[110] Upon review, the Supreme Court held that the warrantless search and seizure of the digital contents of a cell phone is unconstitutional under the Fourth Amendment.[111] The Court found that traditional justifications for a search, harm to officers, and destruction of evidence did not exist with searches of digital data.[112] Moreover, the Court emphasized that cell phones contained "vast quantities of personal information" that could not be compared to a brief physical search.[113] Though the *Riley* case was about a non-border search, it did deal with another Fourth Amendment exception—search incident to arrest.[114] Moreover, the case illuminates the fact that the Supreme Court gives greater deference to privacy interests where digital data is involved.[115] Since the decision, other courts have applied *Riley* in the context of border searches.[116] In *United States v. Smith*, the Southern District of New York drew upon the logic in *Riley* and held that the border search exception does not apply to digital information on a traveler's cell phone because "the magnitude of the privacy invasion caused . . . would allow the government to extend its border search authority well beyond the border itself."[117]

4. Recent Trends & the Evolution of Privacy Norms Online

The Supreme Court's decision in *Carpenter* illustrates that the Court is willing to endorse a more expansive understanding of the reasonable expectations of privacy amidst new technologies being leveraged for invasive purposes.[118]

Another force driving the widened understanding of what constitutes a "search" is the "mosaic theory" of the Fourth Amendment, which was first introduced in *United States v. Maynard*. [119] The mosaic theory essentially

109. *See* Riley v. California, 573 U.S. 373, 378–79 (2014).

110. *See id.* at 379–80.

111. *See id.* at 401.

112. *See id.* at 386.

113. *Id.* at 386.

114. *See id.* at 392 (stating that "the fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely . . . ").

115. Riley v. California, 573 U.S. 373, 392 (2014) (quoting Maryland v. King 569 U.S. 435, 463 (2013)) (stating that " . . . when privacy-related concerns are weighty enough . . . a search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee").

116. *See* United States v. Smith, 673 F. Supp. 3d 381, 394 (S.D.N.Y. 2023).

117. *Id.*

118. *See, e.g.*, *Carpenter*, 585 U.S. at 313; *see generally Jones*, 565 U.S. 400.

119. Matthew B. Kugler & Lior J. Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 206 (2015) (explaining that the mosaic theory was first articulated by Justice Douglas Ginsburg of the D.C. Circuit and served as a stark contrast to prior Fourth Amendment thinking until the Supreme Court embraced it in United States v. Jones).

conducts a Fourth Amendment analysis that assesses a search by observing a series of police surveillance attempts over time rather than examining each discrete police action for whether it in itself qualifies as a search.[120] Taken together, each bit of information aggregated from each surveillance attempt creates a "collective mosaic" that can be quite revealing.[121] So, even if individual steps do not constitute a search, taken together as a mosaic, they may collectively count as a search.[122] Since *Maynard*, in *U.S. v. Jones*, Justice Alito and Justice Sotomayor's concurrences appeared to also endorse the mosaic theory by acknowledging privacy concerns arising from data aggregation.[123] This continues to be a relevant issue today, with machine learning and automated technology tools that can render data analysis and aggregation a quick task.[124]

With respect to privacy on online platforms, some scholars frame privacy settings as "offers" by the website to protect certain pieces of information in a way that induces reliance upon users.[125] Privacy scholar Woodrow Hartzog has argued that privacy features should be construed as enforceable promises and courts should recognize their impact on a user's privacy expectations.[126] While this Note is not specifically focused on the application of contract law principles to the privacy context, the abundance of scholarship supporting the notion that user behavior is influenced by the constraints companies set qualitatively figures into this Note's argument that users may retain privacy expectations while participating on social media platforms.[127]

In fact, lower courts seem increasingly willing to recognize additional factors in the digital realm that inform a user's privacy expectations—like the presence of modifiable privacy settings on social media platforms.[128] However, there is no clear consensus on how much and in what ways users may secure their privacy settings to retain a reasonable expectation of privacy. Some courts have held that a defendant must be able to show that their social media account applied privacy settings that prevented *anyone* from accessing their account information to prove they held a reasonable expectation of privacy and receive Fourth Amendment protections.[129] The court's justification for imposing this high bar is largely because of their adherence

120. *See* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313–14 (2012).

121. *Id.*

122. *See id.*

123. *See Jones*, 565 U.S. at 415-16, 427-30.

124. *See* Daniel J. Solove, *The Limitation of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 991 (2023).

125. Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1652 (2011).

126. *See id.*

127. *See generally* Matthew Tokson & Ari Ezra Waldman, *Social Norms in Fourth Amendment Law*, 120 MICH. L. REV. 265, 300 (2021); *see also* Hartzog, *supra* note 125.

128. *See* United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *6 (D. Conn. July 17, 2018); *see* United States v. Adkinson, No. 4:15-cr-00025-TWP-VTW, 2017 WL 1318420, at *5 (S.D. Ind. Apr. 7, 2017); *see* United States v. Meregildo, 883 F.Supp.2d 523, 525 (S.D.N.Y. Aug. 10, 2012).

129. *See* United States v. Devers, 2012 WL 12540235, at *2 (N.D. Okla. Dec. 28, 2012).

to the misplaced trust and third-party doctrines. For example, in *U.S. v. Meregildo*, the defendant, a Facebook user, argued that they had a reasonable expectation of privacy over their social media data because they tailored their privacy settings to only allow "friends" to view their posts.[130] Though the court agreed a defendant could potentially retain a reasonable expectation of privacy on social media by way of privacy settings, the court declined to find this privacy interest here because the defendant had "no justifiable expectation his friends would keep his profile private . . . because those friends were free to use the information however they wanted—including sharing it with the government."[131]However, other courts have taken the opposite view—finding that individuals who modify their social media privacy settings to share only with "friends" do in fact maintain a reasonable expectation of privacy.[132] For example, in *United States v. Chavez*, law enforcement officers searched a defendant's Facebook account for evidence of a fraudulent telemarketing scheme. In this case, the defendant allowed public access to some content on his social media page (e.g., his name), but he limited access to other content to just himself or his Facebook friends because there were some things "he did not want 'a member' of the general public . . . who was not a 'Facebook Friend'" to see.[133] The court found that the defendant's action to exclude the public from certain content demonstrated that "he maintained a subjective expectation of privacy in that content."[134] The Government attempted to argue, drawing from the misplaced trust doctrine, that the defendant had no reasonable expectation of privacy because the content restricted to friends was shared with hundreds of people, "many of whom . . . he barely had a relationship with."[135] The court rejected this argument outright, warning that dangerous implications could result from courts being the arbiters of whether interpersonal relationships are "sufficiently meaningful."[136] Moreover, the court noted that accepting the Government's argument would be "contrary to the Framers' intention to secure the privacies of life against arbitrary power."[137]

Other courts have also drawn attention to the Fourth Amendment's particularity requirement that any necessary searches should be as limited as possible when constructing a social media user's expectation of privacy.[138] In *United States v. Blake*, a defendant asserted that the FBI's warrant to search their Facebook account was overbroad and violated the Fourth Amendment's particularity requirement because, as the court observed, it "required disclosure to the government of virtually every kind of data that could be found in a social media account."[139] The court agreed with the defendant, finding that the warrants could have been limited to specific messages and

130. *See* United States v. Meregildo, 883 F.Supp.2d 523, 525 (S.D.N.Y. Aug. 10, 2012).
131. *Id.*
132. *See* United States v. Chavez, 423 F.Supp.3d 194, 205 (W.D.N.C. 2019).
133. *Id.* at 202.
134. *Id.*
135. *Id.* at 204.
136. *Id.*
137. *Id.*
138. *See* United States v. Blake, 868 F.3d 960, 973–74 (11th Cir. 2017).
139. *Id.*

periods of time where the defendant was suspected of committing the crime at issue.[140] Moreover, the court noted that such a broad search would be the Internet-era version of a "general warrant," the "abhorred" colonial-era instrument allowing for excessive rummaging of people's belongings.[141]

III. ANALYSIS

The first part of this Note has provided an overview of the key federal agencies involved in implementing different social media surveillance initiatives on immigrants today. It has also outlined the relevant Fourth Amendment jurisprudence illustrating how courts have interpreted individual privacy protections amidst technological advancements that have enabled easier surveillance. The latter half of this Note will apply the Fourth Amendment framework to the social media surveillance landscape. With a focus on the Supreme Court's decision in *Carpenter*, this Note will advance the argument that courts should adopt a more expansive view of the Fourth Amendment to uphold privacy protections when social media surveillance tactics are most aggressive. Moreover, this section will shed light on the low efficacy of modern social media surveillance programs to further support the assertion that adopting a more privacy-protective view in this context would not inappropriately impose upon the interests of law enforcement.

A. Why All Social Media Data Should Not be Considered Wholly "Public"

As outlined in the previous section, many factors may play a role in a court's decision of whether a search or seizure offends an individual's privacy rights under the Fourth Amendment. However, determining whether the information gathered is "public" or "private" in nature typically plays a leading role in the analysis of whether an individual has a reasonable expectation of privacy.[142]

This section will argue that individuals' social media data can be understood as private information deserving of adequate privacy protections for two reasons. First, "social media data" is a broad term encompassing a wide range of information we ordinarily recognize as "personal." Second, the design of social media platforms and modifiable privacy settings encourage users to expect that their data is private and not accessible to law enforcement.

In *Katz*, the 1967 case that created the "reasonable expectation of privacy test," the Court explicitly stated that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[143] Therefore, counterarguments that suggest individuals do not have a privacy interest because social media platforms are inherently "public" do not adequately capture the issue at hand. Not *all* user behavior on social

140. *See id.*
141. *Id.* at 973.
142. *Katz*, 389 U.S. at 351–52.
143. *Id.*

media is public and broadcast to all users in the digital world to take note of. The reality is that an individual's "social media data" consists of more than just the text and images they voluntarily share on a public profile.[144] In fact, mining social media data enables the collection of user information like personal identifiers and demographics (e.g., age, gender), location data (e.g., current address, places visited), user engagement on the platform (e.g., likes, comments, reposts), and personal associations (e.g., "friends," people and pages a user "follows").[145] As discussed earlier, it is important to note that social media platforms have expanded to use cases that do not involve socializing and interacting with others. Therefore, to adequately understand privacy interests on social media platforms, user behavior and expectations must be central to the inquiry.

Oftentimes, a user's behavior online can explicitly or implicitly indicate their manifested intention to remain "private." The most obvious example is when individuals create a social media profile that is intended to be private from the start—opting for a de-identified username and/or making the conscious choice to avoid posting any content of their own, particularly anything that may reveal personal identifying information. Even when a user's profile is public, this may not automatically mean that the user has chosen to make *all* their activity on the platform public. Most social media platforms offer a range of privacy settings that may inform users' expectations of their privacy rights.[146] These privacy settings are typically separate from the platform's privacy policies and allow users to customize who can access specific content they post, view their activity, and more.[147] By taking active steps to customize their privacy settings, users are arguably exhibiting a desire to maintain their privacy online.

As illustrated by *Meregildo* and *Chavez*, lower courts that have had the opportunity to address Fourth Amendment protections with respect to social media searches and are willing to recognize that privacy settings can impact social media users' expectations of privacy.[148] While the *Meregildo* and *Chavez* courts diverged about whether a user modifying privacy settings to "friends only" meant an individual "lost" their reasonable expectation of privacy, these cases are still consistent. Both courts examined the role privacy settings played when conducting their Fourth Amendment analysis and in

144. *See* Alexandra Mateescu et.al, *Social Media Surveillance and Law Enforcement*, DATA C.R. 1, 2–4 (Oct. 27, 2015), https://datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf [https://perma.cc/Y55L-BKWC]; *see* Adrian Shahbaz & Allie Funk, *Social Media Surveillance*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance [https://perma.cc/36UY-RNQT] (last visited Jan. 27, 2024)**;** *see Social Media Data Mining: Understanding What It Is and How Businesses Can Use It*, U. SAN DIEGO (Apr. 3, 2020), https://www.sandiego.edu/blogs/business/detail.php?_focus=76022 [https://perma.cc/MVD3-VNBC].

145. *See generally* Mateescu et.al, *supra* note 144; Shahbaz & Funk, *supra* note 144.; *Social Media Data Mining*, *supra* note 144.

146. *See* Thorin Klosowski, *Simple Online Security for Social Media Accounts*, N.Y. TIMES (Apr. 22, 2022), https://www.nytimes.com/wirecutter/guides/online-security-social-media-privacy/ [https://perma.cc/9VQA-9H8F].

147. Hartzog, *supra* note 125.

148. *See, e.g.*, *Meregildo*, 883 F.Supp.2d at 525; *see Blake*, 868 F.3d at 973–74; *see also Westley*, 2018 WL 3448161, at *6; *see also Adkinson*, 2017 WL 1318420, at *5.

formulating whether the defendant retained a reasonable expectation of privacy.[149]

When the concept of a "reasonable expectation of privacy" was created, it was intended to be informed by social norms.[150] However, as Justice Alito contemplated in his concurrence in *Jones*, the reasonable expectation of privacy test is prone to circular reasoning, and judges may be confusing their own expectations of privacy instead of the hypothetical reasonable person.[151] Alternatively, as legal and privacy scholars Matthew Tokson and Ari Waldman posit, individual actors do not create norms, but rather, norms are shaped by companies and the product design they promote.[152] Consequently, social media users can only exert their privacy interests within the constraints that platforms *allow* them to. The reasonable expectation of privacy test rests on the assumption that privacy expectations are stable, but technology can change those expectations.[153] For the ordinary social media user, the only way to exercise control over their privacy after signing up for an account is by utilizing the platform's customizable privacy settings. Courts have already been affirmatively expressing support for the evolving nature of the Fourth Amendment for years.[154] Therefore, it is within the courts' power to understand and apply the Fourth Amendment in the context of subjective user privacy expectations informed by the reality of social media platforms.

Many credit the "beginning of social media" to 2004 when MySpace reached one million active monthly users.[155] Since then, social media has become a dominant force in the digital world.[156] The rapid growth of social media platforms has been likened to other recognized communication-enabling technologies like computers, smartphones, and the Internet.[157] Today, the most popular social media platforms, like Facebook, YouTube, and WhatsApp, each host over one billion users and have sustained themselves for over ten years.[158] Because the Fourth Amendment protects people, not places, its protections must extend to the number of individuals active on social media platforms every day.[159]

Given the fact that social media platforms hold such a crucial position in modern-day communication, and there are both privacy and free speech interests at stake here, the third-party doctrine should not be applied without recognition of the reality of what it means to be an online user in today's

149. *See Meregildo*, 883 F.Supp.2d at 525–26; *see Chavez*, 423 F.Supp.3d at 201–02.

150. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (noting that an expectation of privacy must be "one that society is prepared to recognize as 'reasonable'").

151. *See Jones*, 565 U.S. at 427.

152. *See* Tokson & Waldman, *supra* note 127, at 300.

153. *See Jones*, 565 U.S. at 427 (Alito, J., concurring).

154. *See, e.g.*, Warshak v. United States, 631 F.3d 266, 286 (6th Cir. 2014) (noting that "as some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise").

155. Esteban Ortiz-Ospina, *The Rise of Social Media*, U. OXFORD (Sept. 18, 2019), https://ourworldindata.org/rise-of-social-media [https://perma.cc/66X7-AVEU].

156. *Id.*

157. *See id.*

158. *See id.*

159. *See Katz*, 389 U.S. at 351.

digital world. Even in 1979, when *Smith v. Maryland* was decided, Justice Marshall noted in his dissent that "privacy is not a discrete commodity, possessed absolutely or not at all."[160] Moreover, in recent years, the Supreme Court seems more receptive to criticisms of the third-party doctrine applied online. For example, in her concurrence in *U.S. v. Jones*, Justice Sotomayor noted that the doctrine needed to be reconsidered because people are presently forced to provide information about themselves to third parties for even the most mundane tasks.[161]

B. Extensive Data Collection Post-Carpenter

This section will describe how the Supreme Court's decision in *Carpenter v. United States* signals a shift away from a rigid application of the third-party doctrine and argue that *Carpenter* should have a cognizable impact on how courts understand individual privacy interests on social media. First, this section will examine the Supreme Court's holding in *Carpenter* and the boundaries the Court set in determining the scope of its decision. Next, it will illustrate how law enforcement's aggressive social media surveillance tactics satisfy several of these factors such that the third-party doctrine should not bar the Fourth Amendment's application in this context.

Though *Carpenter* expanded the Fourth Amendment's protections, the Court specifically emphasized that the decision was limited to CSLI data, did not eliminate the third-party doctrine, and should not be interpreted to question traditional surveillance tools, like security cameras.[162] Despite the Court's efforts to define the scope of its decision, it did not specifically provide a test for future courts to apply in deciding what qualifies as comprehensive data collection. Therefore, the decision ultimately still raises considerations for similar kinds of data collection that could also be found too extensive to fall within the bounds of the third-party doctrine.

As noted earlier, the six factors gleaned from *Carpenter* to determine whether surveillance is exempt from the third-party doctrine are: how revealing the data is, the amount of data collected, the number of people affected, the inescapable nature of the surveillance, whether the disclosure of data to the third party is automated, and the difficulty of conducting surveillance.[163] The social media surveillance techniques law enforcement have employed on immigrants arguably qualify as extensive based upon four factors—revealing nature of data, amount of data collected, number of people affected, and difficulty of conducting surveillance.

First, social media data is "revealing" in a manner acknowledged by the *Carpenter* court. In *Carpenter*, the Court found location information to be particularly sensitive because it also revealed "familial, political, professional, religious, and sexual associations" that ultimately represented "privacies of life."[164] Similarly, social media data contains extensive personal

160. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).
161. *Jones*, 565 U.S. at 417 (Sotomayor, J. concurring).
162. *See Carpenter*, 585 U.S. at 298.
163. *See id.* at 339-40.
164. *See id.* at 311.

information—from basic identifiers (e.g., name, age, and address) to location data (e.g., current location, businesses frequented), and information about an individual's relationship status, political affiliations, and religious beliefs that may be directly or indirectly gleaned from their activity on the platform.[165] Additionally, even DHS has categorized social media handles as sensitive personally identifiable information.[166]

Data aggregation is a recognized privacy concept that illustrates why social media surveillance can be so revealing and invasive. This concept describes the phenomenon where individual data points seem trivial but actually become more powerful and invasive of privacy when linked together to form a bigger picture.[167] Data aggregation is the basis for the mosaic theory of Fourth Amendment analysis that has become increasingly recognized after *Jones* and *Carpenter*.[168] In the context of social media monitoring, data aggregation explains why machine learning and analytical tools used by law enforcement can be so invasive. For example, during border searches, after extracting social media data from cell phones, ICE runs collected information through an analytical tool, FALCON-SA, that is capable of conducting a "social network analysis."[169] The produced analysis highlights trends and draws connections between different people, businesses, and ICE investigations based upon a combination of collected social media data and other information from separate ICE and CBP databases.[170] Moreover, the agency is authorized to not only access data, but also store and share it with other law enforcement agencies.[171]

Personal data is interrelated to begin with because "life involves relationships and transactions between people."[172] AI and machine learning tools only further facilitate our ability to interrelate people.[173] ICE's social network analysis tool, which is capable of drawing connections between people, is an illustrative example.[174] This also highlights the fact that the value of social media monitoring is not gathering information about a singular person, but rather gathering information about *many* people the analytical tool deems to be closely affiliated with an individual. Consequently, though law enforcement may be targeting recent immigrants, long-time American citizens are effectively being surveilled too because their information is

165. *See generally* Samuel Wamba et al., *The Primer of Social Media Analytics*, 28 J. ORGANIZATIONAL & END USER COMPUTING 1 (2016).

166. *See* Rachel Levinson-Waldman et al., *Social Media Surveillance by the U.S. Government*, BRENNAN CTR. JUST. (Jan. 7, 2022), https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government [https://perma.cc/KH96-3G4W].

167. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1889–90 (2013).

168. *See* Kugler & Strahilevitz, *supra* note 119, at 205–08.

169. Patel et al., *supra* note 12, at 15.

170. *See id.* at 16.

171. *See id.* at 27.

172. Solove, *supra* note 124, at 990.

173. *See id.* at 991.

174. *See* Patel et al., *supra* note 12, at 15–16.

indirectly analyzed and stored in law enforcement databases.[175] In *Carpenter*, the Court left open the question of whether "collection techniques involving foreign affairs or national security" fell within the scope of its holding. However, given that the scope of surveillance may be so wide, sometimes bleeding into the lives of average American citizens, arguably comprehensive monitoring cannot always be appropriately categorized under the umbrella of foreign affairs.

The scope of surveillance also further relates to the next *Carpenter* factor regarding the amount of data collection at issue. Social media monitoring may result in a large amount of data collection from a significant number of people, depending on the circumstances. Surveillance tactics that rely on "continuous" monitoring have the capacity to amass a significant amount of data.[176] One example is ICE's contract with Giant Oak, a data mining firm, to implement a surveillance program that continuously monitors visa applicants from the time of submission.[177] Visa applicants' social media data was then aggregated and analyzed to evaluate behavioral patterns and ultimately aid in enforcing its Overstay Lifecycle program.[178] A similar technique is used during the course of a border search. When ICE accesses a digital device during a border search, it can currently extract information from the device if the data is "pertinent" to an investigation or enforcement activity.[179] As previously discussed, once social media data is extracted from the device, it is processed through FALCON-SA for analysis and ultimately generates an in-depth report on findings.[180] It is also worth noting that in circumstances where ICE relies on human-driven monitoring, instead of machine learning and AI, the surveillance is arguably still extensive. For example, in 2018, ICE spent $100 million to hire 180 people to monitor 10,000 "high-risk" foreign visitors continuously throughout their stay in the United States, only ceasing efforts if the visitor is granted legal residency.[181]

The existence and use of machine learning surveillance programs are also responsive to the *Carpenter* factor regarding the difficulty of conducting surveillance. This factor essentially provides that where the time and effort required for surveillance is low, the more likely it is to be considered a search because it is more prone to abuse, overuse, and less administrative or political scrutiny.[182] Additionally, many privacy scholars discussing mass surveillance initiatives point to the "quantitative privacy" concerns these programs

175. *See id.* at 29.

176. Patel et al., *supra* note 12, at 7–8; *see* Shaiba Rather & Layla Al, *Is The Government Tracking Your Social Media Activity?*, ACLU (Apr. 24, 2023), https://www.aclu.org/news/national-security/is-the-government-tracking-your-social-media-activity [https://perma.cc/3RPF-4WWY] (discussing a DHS program that monitored non-citizens from the time they apply for an immigration benefit to when they become a naturalized citizen).

177. *See* Cox, *supra* note 53.

178. *See id.* (explaining how ICE has expanded its use of AI-powered tools to more generally surveil social media for posts containing derogatory comments).

179. *See* Patel et al., *supra* note 12, at 27.

180. *See id.* at 28.

181. *See id.* at 26.

182. *See* Tokson, *supra* note 104, at 1804.

raise.[183] Privacy law scholars David Gray and Danielle Citron assert that what matters most for Fourth Amendment analysis is the *means* of surveillance.[184] Therefore, privacy interests are implicated where surveillance is "broad and indiscriminate" because these conditions enable a surveillance state.[185] In the social media context, the machine learning tools ICE utilizes allow for bulk screening programs that operate with high efficiency, analyzing data from a mass amount of people and providing synthesized reports for law enforcement.[186]

C. Is Modern Social Media Surveillance Effective?

A common theme underlying Fourth Amendment cases is the tension between privacy interests and the interests of law enforcement and national security. However, both privacy and national security are important values for the greater public welfare, and the Supreme Court has recognized that each represents strong values that should not be compromised.[187] However, law enforcement's proposed and implemented social media surveillance tactics thus far are aggressive and largely extinguish the privacy interests of immigrants altogether. Despite the extensive nature of surveillance, it is questionable, at least to this author, just how beneficial this surveillance really is for national security purposes.

First, there is an abundance of research finding that there is no single indicator or profile that can affirmatively predict if someone is a terrorist.[188] Therefore, law enforcement's practice of monitoring social media for "hints" of the risk someone poses to the nation seems questionable. Moreover, law enforcement officials themselves seem to be skeptical of how useful social media surveillance actually is.[189] An email chain between staff at the Office of the Director of National Intelligence indicated that staff members believed collecting social media identifiers was useless and added no value to the immigration screening process.[190] Additionally, the 2016 report from the DHS

183. Danielle Citron & David Gray, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 73–75 (2013).

184. *See id.* at 71–72.

185. *Id.*

186. *See* Patel et al., *supra* note 12, at 25–28.

187. *See* United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 321 (1972) (stating that national security interests do not categorically trump individual privacy and free expression).

188. *See, e.g.*, Faiza Patel, *Rethinking Radicalization*, BRENNAN CTR. JUST. 8–10 (Mar. 8, 2011), https://www.brennancenter.org/our-work/research-reports/rethinking-radicalization [https://perma.cc/HG8K-J9VT]; *see* Levinson-Waldman et al., *supra* note 160 (noting that social media conversations are difficult to interpret and "[g]overnment officials and assessments have repeatedly recognized that this dynamic makes it difficult to distinguish a sliver of genuine threats from the millions of everyday communications that do not warrant law enforcement attention"); *see generally* Timme Bisgaard Munk, *100,000 False Positives for Every Real Terrorist: Why Anti-Terror Algorithms Don't Work*, FIRST MONDAY (Sept. 2017), https://firstmonday.org/ojs/index.php/fm/article/view/7126/6522 [https://perma.cc/TJV5-TPB7].

189. *See State Department Rule Ineffective*, *supra* note 48.

190. *See id.*

Office of the Inspector General explicitly stated that ICE's pilot programs lacked adequate metrics and recommended that USCIS and ICE focus more efforts on evaluating initiatives.[191]

IV. RECOMMENDATIONS

Technology has enabled law enforcement to monitor immigrants and impinge upon their privacy without any real consequence or mechanism for accountability. Despite little evidence supporting the notion that social media surveillance is effective, law enforcement continues to engage in social media surveillance in various ways.[192] As previous sections have described, some examples include requesting social media handles on visa applications, extracting digital data at the border, and working with private entities to utilize advanced data analytics tools powered by mass data aggregation and automated monitoring.[193] There are serious privacy concerns at stake and revamping this system requires interventions at both the legal and policy level. Therefore, this section will (1) argue that law enforcement should be required to obtain a warrant before engaging in specific forms of social media surveillance, and (2) advocate for a process requiring more transparency from law enforcement agencies engaging in social media surveillance.

First, this Note argues that after the Supreme Court's decision in *Carpenter*, there are specific forms of social media surveillance that should require law enforcement to obtain a warrant prior to use. As discussed, the *Carpenter* factors highlight various elements that can make surveillance particularly aggressive and thereby exempt from the third-party doctrine.[194] The revealing nature of data, the volume of data collected, the large number of individuals affected, and the relative ease of conducting surveillance are all implicated in the social media surveillance context. For example, surveillance techniques relying on machine learning and automated monitoring often enable law enforcement to engage in continuous monitoring over a period of time.[195] Moreover, the sophisticated nature of this technology likely allows law enforcement to screen vast quantities of data at a rate exceeding manual screening.

Even under *Carpenter*, many invasive social media surveillance practices would not be deemed aggressive enough to require law enforcement to obtain a warrant. Examples might include where law enforcement looks up an individual's public social media page or where a law enforcement agent goes undercover to befriend an individual on social media for information-gathering purposes. These are ultimately human-driven processes that do not respond to the concerns raised by *Carpenter* about technology being leveraged to make surveillance broad, cheap, and quick.[196]

---

191. *See DHS Social Media Screening*, *supra* note 46 ("The OIG's draft report states that the 'pilots did not have metrics to measure success' and 'did not establish […] benchmarks.'").

192. *See* discussion *supra* Section III.C.

193. *See* discussion *supra* Sections II.A.2–3.

194. *See Carpenter*, 585 U.S. at 339-40.

195. *See generally* Patel et al., *supra* note 12, at 8.

196. *See Carpenter*, 585 U.S. at 311-12.

Ultimately, it is important to highlight that requiring law enforcement to obtain a warrant prior to conducting certain kinds of social media surveillance does not automatically resolve privacy concerns on its own. As noted earlier, many of the most aggressive social media surveillance initiatives were pitched as pilot programs, which are not often rigorously evaluated for program efficacy and implementation.[197] This gives way to another problem: a dearth of reporting and publicly available information that brings transparency to the process, goals, and success of these surveillance initiatives. It is difficult to assess the interests at stake and how people's rights are being infringed upon without more transparency.

Therefore, this Note also proposes a policy recommendation aimed at improving transparency from law enforcement agencies about social media surveillance practices. One way this could be achieved is through the PCLOB.[198] As previously noted, federal law enforcement agencies issue reports to PCLOB about their work, and PCLOB regularly publishes its own reports detailing recommendations on various surveillance issues.[199] For example, there could be a mandatory reporting obligation imposed on law enforcement agencies to provide information about new pilot programs, particularly those employing machine learning and automated decision-making tools. This information would ideally provide insight concerning program implementation, data retention practices, and any metrics evaluating program efficacy. Moreover, the PCLOB could advise agencies on how to design programs to be more privacy-conscious and publish reports on an agency's compliance with privacy principles for public transparency.

Another policy recommendation is for Congress to impose more transparency obligations for social media platforms in responding to law enforcement's requests for user data. While some social media companies, like Meta, already voluntarily publish a range of metrics related to law enforcement's requests for information, it is unclear whether all platforms are required to do so by law.[200] Setting a standardized list of metrics that platforms are required to provide would also help policymakers have a better grasp of surveillance trends and make it easier for users to understand their privacy risks across platforms. Additionally, platforms could be required to provide more insight into their internal processes for determining whether an information request from law enforcement is adequate. Finally, social media companies could be required to provide some level of notification to users if their data is requested where not otherwise legally prohibited.

V. CONCLUSION

Social media surveillance is a civil liberties issue that significantly impacts the privacy rights of both recent immigrants and Americans. This

197. *See* Patel et al., *supra* note 12, at 26.; *see DHS Social Media Screening*, *supra* note 46.

198. *See* discussion *supra* Section II.A.1.

199. *See id.*

200. *See, e.g.*, *Government Request for User Data*, *supra* note 86.

issue is only becoming more pressing with the rise of automated tools that make it easier and cheaper for law enforcement to extract an abundance of information about an individual that goes far beyond the traditional notion of a Fourth Amendment search. Over the years, courts have consistently recognized the need for the Fourth Amendment to keep up with the latest technology and surveillance tools. Due to aggressive, warrantless surveillance, there needs to be judicial recognition that immigrants using social media have justifiable expectations of privacy on platforms. As the number of participants on social media platforms grows, it is important to prioritize individual privacy rights in Fourth Amendment interpretation to keep up with an expanding cyberspace.