THINK BEFORE YOU POST: SOCIAL MEDIA MONITORING OF IMMIGRANTS AND IMPLICATIONS ON CONSTITUTIONAL RIGHTS AND DISCRIMINATORY DENIALS

Brooke Gary*

I. Introduction

Individuals interested in applying for a United States ("U.S.") visa or immigration benefit, seeking asylum or refugee status, or becoming a U.S. permanent resident or citizen, now need to think twice before their next post or interaction on social media.1 When a foreign national seeks to enter the U.S., they are required to provide biographical and personal information including their names, birthdate, addresses, and education and employment information to...
United States Citizenship and Immigration Services (“USCIS”), the federal agency that oversees lawful immigration to the U.S. The Department of Homeland Security (“DHS”) implements U.S. immigration law and policy through USCIS' processing and adjudication of immigration applications and petitions submitted for citizenship, asylum, and other immigration benefits. As a foreign

See Susan Miller, Monitoring Migrants in The Digital Age: Using Twitter to Analyze Social Media Surveillance, 17 COLO. TECH. L.J. 395, 396 (2019) (explaining that visa applications require biographical and personal information including names, addresses, birthdates, work addresses, job titles, and education information). See also Chapter 7 - Privacy and Confidentiality, U.S. CITIZENSHIP & IMMIGR. SERVS. (Oct. 1, 2021), archived at https://perma.cc/WG5X-YUZQ (listing personally identifiable information that USCIS collects, uses, and maintains to include name, address, date of birth, social security number, driver’s license number, passport number, and biometric identifiers); Filling Out the Application for U.S. Citizenship, CITIZEN PATH (May 21, 2019), archived at https://perma.cc/M39E-7V9F (describing information requested in U.S. Citizenship applications, including name, information about your residence, parents, children, employment and educational institutions, travel outside the U.S., and marital history). See also What We Do, U.S. CITIZENSHIP & IMMIGR. SERVS. (Feb. 27, 2020), archived at https://perma.cc/8J8N-5YXP (noting that USCIS is the federal agency that oversees lawful immigration to the U.S.). See also Brief of the Alliance of Business Immigration Lawyers, Inc., as Amicus Curiae, in Support of Plaintiffs at 4, Immigrant Legal Res. Ctr. v. Wolf, 491 F. Supp. 3d 520 (N.D. Cal. 2020) (No. 4:20-cv-05883-JSW) (listing the functions of USCIS to be adjudications of immigrant visa petitions, adjudications of naturalization petitions, adjudications of asylum and refugee applications, and adjudications performed at service center). Ultimately, the sole function of USCIS is prescribed as “adjudications” of requests for immigration and naturalization benefits. Id. at 10.

See Tom Murse, Department of Homeland Security History, THOUGHTCO. (Mar. 22, 2021), archived at https://perma.cc/ZTX7-V6PG (defining the DHS as a Cabinet-level department of the U.S. federal government that aims to prevent terrorist attacks in America). President George W. Bush created DHS in response to the attacks of September 11, 2001, and with the goal of making Americans safer. Id. See also Operational and Support Components, HOMELAND SEC. (Oct. 16, 2021), archived at https://perma.cc/4W7N-69W5 (listing the Operational and Support Components that currently make up the Department of Homeland Security, including USCIS). USCIS administers the nation’s lawful immigration system and safeguards its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits. Id. See also U.S. Dep’t of Homeland Sec., Privacy Impact Assessment for the Computer Linked Application Management System and Associated Systems (CLAIMS 3), DHS/USCIS/PIA-016(d) (June 30, 2020) [hereinafter Privacy Impact Assessment] (outlining actions taken by USCIS after receiving an immigration form or application). “Once a benefit request form is submitted to USCIS, a series of processing and adjudication actions occur, such as

While USCIS continues to collect each foreign national’s demographic information to conduct their respective background checks and store in their A-file, the federal government is now also reviewing and storing information related to a foreign national’s social media footprint, including the content they share online, their interactions, and their network of associations.5
Recent enacted policies and policy proposals by the DHS and the U.S. State Department allow USCIS officers to collect, monitor, and retain information on a foreign national’s online activity before rendering a decision on their immigration application.\(^6\)

The DHS and State Department claim that they gather data from social media as an effort to combat national security threats and results); V. Blue, *Americans are horrified by DHS plan to track immigrants on social media*, ENGADGET (Sept. 29, 2017), archived at https://perma.cc/XG3Y-38TA (noting that A-files on immigrants will now include “all kinds of information gleaned both directly and indirectly from social-media profiles.”). See also Faiza Patel, *Stop Collecting Immigrants’ Social Media Data*, BRENANN CTR. JUST. (June 30, 2019), archived at https://perma.cc/ZY7F-AJ5N [hereinafter *Stop Collecting Immigrants’ Social Media Data*] (describing how DHS is finding ways to use social media data in several programs). The DHS has conducted searches of phones and laptops at the border and checks of people applying for visas and immigration benefits. Id. See also Brian Rotsztein, *Managing Your Social Media Footprint*, SOC. MEDIA TODAY (Apr. 4, 2013), archived at https://perma.cc/5KZL-ZGZ4 (defining a social media footprint as the trail that you leave behind for others to find every time you upload a photo on Instagram, share anything on Facebook, tweet on Twitter, publish videos of yourself on YouTube, add jobs and education info on LinkedIn, and so on). Despite what you might think, even if what you post online is motivated through an emotionally charged moment of happiness, excitement, or anger, people will take what you post as a real opinion. Id. See also WHAT’S YOUR SOCIAL MEDIA FOOTPRINT AND WHY DOES IT MATTER?, DIGIT. MKTG. JOBS (May 25, 2021), archived at https://perma.cc/96ZT-S3M7 (emphasizing that all engagement on social media is recorded and archived and everything you read, view, say, buy, and search leaves a trail that can be revisited by others). A social media footprint also contains a person’s network of associations to different people, groups, and ideas that they have created for themselves. Id. Every time someone has liked, commented on, or shared something, it has been recorded and used. Id.

\(^6\) See Exec. Ord. No. 13780, 82 Fed. Reg. 13209, 13215 (Mar. 6, 2017) [hereinafter Exec. Ord. 13780] (directing a series of actions to enhance the security of the American people, including raising the baseline for the vetting and screening of foreign nationals). See also Tim Lau, *The Government Is Expanding Its Social Media Surveillance Capabilities*, BRENANN CTR. JUST. (May 22, 2019), archived at https://perma.cc/FY4J-JVUR (describing how federal government agencies such as the DHS have expanded their social media monitoring programs and are collecting a vast amount of user information). The DHS uses information collected for vetting and analysis for individuals seeking to enter the U.S. Id. See also Harsha Panduranga, *Social Media Vetting of Visa Applicants Violates the First Amendment*, BRENANN CTR. JUST. (Dec. 9, 2019), archived at https://perma.cc/ZZA4-UCUR (explaining that the State Department has required almost everyone applying for a U.S. visa to register every social media username they have used over the past five years). Once obtained, the username information is then retained indefinitely. Id.
counterterrorism.⁷ Although social media can provide quick insight into an individual’s personal information, interests, and behaviors, online identities are fluid and subject to interpretation, and it is questionable just how effective social media vetting of immigrants is in identifying national security threats.⁸ The use of social media

⁷ See Miller, supra note 2, at 398 (stating that social media surveillance and data collection have found their way into the U.S.’s toolbox for national security); Faiza Patel et al., Social Media Monitoring, BRENAN CTR. FOR JUST. (Mar. 11, 2020), archived at https://perma.cc/N6U8-PGRD [hereinafter Social Media Monitoring] (explaining that DHS personnel are examining “social media to identify information related to undefined ‘national security’ risks or concerns.”). See also Jackie Bischof, The US Just Added One More Requirement for Visa Applicants to Stress About, QUARTZ (July 20, 2022), archived at https://perma.cc/TR4W-WSV3 (outlining the State Department’s view that “[s]ocial media can be a major forum for terrorist sentiment and activity”). Social media monitoring will be a “vital tool to screen out terrorists, public safety threats, and other dangerous individuals from gaining immigration benefits and setting foot on US soil.” Id. See also U.S. Dep’t of State, Supporting Statement for Paperwork Reduction Act Submission 13 [hereinafter Supporting Statement] (stating that national security is the government’s top priority when adjudicating visa applications). “Maintaining robust screening standards for visa applicants is a dynamic practice that must adapt to emerging threats.” Id.

⁸ See Jiao Huang et al., A Literature Review of Online Identity Reconstruction, FRONTIERS PSYCH. (Aug. 23, 2021), archived at https://perma.cc/G44R-MREH (suggesting that an individual’s identity in the online world may be different from his or her offline identity). “Some people may reconstruct their identity on the Internet to build an online identity that is partly or even completely different from their real identity in the offline world.” Id. See also Social Media Monitoring, supra note 7 (explaining that it is difficult to determine “with any level of certainty” the “authenticity, veracity, [or] social context” of social media data). While social media can provide a great deal of information about individuals, such as their personal preferences, political ideologies, religious views, physical and mental health, and the identity of their friends and family, it is also susceptible to misinterpretation. Id. See also Manar Waheed, New Documents Underscore Problems of ‘Social Media Vetting’ of Immigrants, ACLU (Jan. 3, 2018), archived at https://perma.cc/G8H6-575P (presenting findings from social media vetting pilot programs which indicated that attempts at social media vetting produced few to no results, with only a smattering of posts flagged, even though the threshold for flagging was low); POGO Urges DHS to Abandon Problematic Social Media Collection Plan, POGO (May 31, 2018), archived at https://perma.cc/JW7V-SELT (emphasizing that social media communications have context-specific meanings that are notoriously difficult to interpret, and as a result are more apt to raise false positives than to identify real security threats).
monitoring has also been heavily challenged and denounced for enabling discriminatory pretextual denials of immigration petitions and infringing on an individual’s Constitutional rights to privacy and free speech and association.9

The DHS and U.S. State Department should cease their practice of collecting, monitoring, and retaining foreign nationals’ social media data. If, however, these practices are to continue, the government should be required to fully disclose details on how they scrutinize a foreign national’s social media and use that data to deny immigration and naturalization attempts. Ultimately, social media can provide information about foreign nationals that is important for national security and public safety, but the wholesale monitoring of social media poses serious risks to the Constitutional rights of both foreign nationals and U.S. citizens and opens the door to discriminatory pretextual denials of immigration applications.

II. History

A. Immigration Monitoring Pre-Social Media Era

Before the existence and widespread use of social media and information technology, it was much more difficult to collect, analyze, and retain large amounts of public information over a long period of

---

9 See Waheed, supra note 8 (describing the ACLU and other civil rights groups’ concern that social media monitoring programs will focus unfairly on Muslim immigrants and immigrants from Muslim-majority countries). “The government is speeding ahead with social media surveillance, without regard for the concerns that have been raised, the integrity of our immigration system, or the civil rights of those impacted – which may include virtually anyone living in America.” Id. See also Social Media Monitoring, supra note 7 (emphasizing that “[p]ersonal information gleaned from social media posts has been used to target dissent and subject religious and ethnic minorities to enhanced vetting and surveillance.”). In addition, social media monitoring creates serious risks to privacy and free speech. Id. Generally, social media monitoring “will impact what people say online, leading to self-censorship of people applying for visas as well as their family members and friends.” Id. See also Dave Nyczepir, DHS sued over social media surveillance of visa holders, FedScoop (Jan. 19, 2021), archived at https://perma.cc/Y5WF-ELMJ (arguing that “[g]overnment monitoring of social media opens the door to discriminatory pretextual denials of benefits and may have the effect of chilling Americans’ speech”).
time for just one person, let alone all foreign nationals.  

Nevertheless, various forms of immigration monitoring and vetting occurred long before the emergence of social media, and were similarly justified as a means of protecting national security. Under the Immigration and Nationality Act of 1952, also known as the McCarran-Walter Act (“the Act”), the government began monitoring and inspecting immigrants and excluding them based on their nationality, political views, and lack of good moral character. While the Act did not specify forms or

10 See Jeramie D. Scott, *ESSAY: Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. BUS. & TECH. L. 151, 154 (2017) (explaining that before the use of information technology, aggregating disparate public records and surveilling the public activities of one individual would have taken a great deal of manpower). See also Adam Glenn, *Doc Society v. Blinken: Challenging the State Department’s Social Media Registration Requirement*, KNIGHT FIRST AMEND. INST. COLUM. UNIV. (Sept. 16, 2021), archived at https://perma.cc/V8ZQ-TYFE (noting that in the past, the government would have had to wiretap millions of homes and offices, meeting houses, and other locations to collect the kind of information that it can now sweep up all at once).

11 See Miller, supra note 2, at 410 (stating that vetting immigrants by the U.S. government is not a new practice). Since 1978, surveillance techniques and restrictions put in place have made the process of immigrating to the U.S. difficult. *Id.* “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.” *Id.* at 399. See also Ruchir Patel, *ARTICLE: Immigration Legislation Pursuant to Threats to US National Security*, 32 DENV. J. INT’L L. & POL’Y 83, 83 [hereinafter *Immigration Legislation Pursuant to Threats*] (explaining that the U.S. relies upon immigration policies to protect itself against subversives, such as spies, saboteurs, anarchists, and terrorists). The protective immigration policies that the U.S. has legislated and implemented have been in response to fear of immigrants who seek to destroy the government rather than strive for the shelter of its freedoms. *Id.* at 84.

12 See *McCarran-Walter Act goes into effect, revising immigration laws*, HIST. (Dec. 21, 2020), archived at https://perma.cc/JWR5-SAN9 (providing that the McCarran-Walter Act was “hailed by supporters as a necessary step in preventing alleged communist subversion in the United States.”). The McCarran-Walter Act permitted more strenuous screening of potential immigrants, by banning admission to anyone declared a subversive by the Attorney General or a member of communist and “communist-front” organizations. *Id.* In addition, the Act continued the quota system for immigration into the U.S., allotting two-thirds of the 154,657 spots available each year to immigrants from Great Britain, Ireland, and Germany and only a small number of spots for immigrants from nations such as Japan and China. *Id.*
means of surveillance, it did allow individuals to be denied entry into the U.S. based simply on their affiliations, speech, and the government’s perception that the foreign national’s views were antithetical to those of the U.S.\textsuperscript{13} In addition, in 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“PATRIOT Act”) expanded surveillance laws and permitted the government to employ surveillance technology that could monitor email, phone, and other types of internet communications of citizens and foreign nationals.\textsuperscript{14} Finally, it is also believed that consular officers have used the option

\textit{See also Immigration Legislation Pursuant to Threats, supra note 11, at 85 (explaining that the McCarran-Walter Act introduced an ideological criterion for admission to the U.S.). Immigrants and visitors to the U.S. could be denied entry on the basis of their political ideology, namely if they were communists. \textit{Id. See also Dobrina Ustun, Significance of Good Moral Character for Naturalization, USTUN L. GRP.} (Dec. 26, 2019), \textit{archived at} https://perma.cc/4TYL-DG7B (noting that under the Immigration and Nationality Act, an applicant for naturalization must establish good moral character). The Act does not directly define good moral character, but it does describe certain acts that bar establishing good moral character, including various forms of fraud, unlawful harassment, obstruction of justice, failure to pay taxes, and conspiracy to distribute a controlled substance. \textit{Id.}\textsuperscript{13}\textit{ See Alexander Wohl, Free Speech and the Right of Entry Into the United States: Legislation to Remedy the Ideological Exclusion Provisions of the Immigration and Nationality Act, 4 AM. U. INT’L L. REV. 443, 444 (1989) (emphasizing that the McCarran-Walter Act granted the U.S. government the far-reaching power to exclude or deport foreign visitors on the basis of their political beliefs, affiliations, or speech). The Act punished the mere writing, publication, or distribution of materials connected with proscribed activities. \textit{Id.} at 457. As a result, citizens, political activists, and scholars argued that the McCarran-Walter Act infringed on first amendment rights. \textit{Id.} at 445.}\textsuperscript{14}\textit{ See Alicia J. Campi, The McCarran-Walter Act: A Contradictory Legacy on Race, Quotas, and Ideology, IMMIGR. POL’Y CTR.} (June 2004), \textit{archived at} https://perma.cc/R4ZA-PJG6 (explaining that although most of the provisions of the McCarran-Walter Act were formally repealed by Congress in 1990, many were resurrected by the PATRIOT Act of 2001). The PATRIOT Act targeted aliens for deportation and exclusion based not on their actions but on their words. \textit{See also SURVEILLANCE UNDER THE PATRIOT ACT, ACLU} (Nov. 12, 2021), \textit{archived at} https://perma.cc/B3B4-CGUQ (stating that the PATRIOT Act was passed in response to 9/11 and in the name of national security). The PATRIOT Act was “the first of many changes to surveillance laws that made it easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit reporting records, and track the activity of innocent Americans on the Internet.” \textit{Id. See also Immigration Legislation Pursuant to Threats, supra note 11, at 89 (noting that the PATRIOT Act expanded the government’s ability to conduct surveillance).}
of searching visa applicants on Google, on an ad hoc basis, as a means of investigating foreign nationals and confirming the validity of information included in their application.15

B. Social Media Monitoring in Immigration – Throughout Past Presidential Administrations

1. The Obama Administration

The practice of collecting a foreign national’s social media information first emerged through various pilot programs enacted under the Obama administration.16 Prior to 2014, a supposed secret U.S. policy prohibited immigration officials from reviewing the social

---

15 See Diane Butler, Visa Applicants Coming to the U.S.? Not Without Disclosing Social Media Handles, DAVID WRIGHT TREMAINE LLP (June 11, 2019), archived at https://perma.cc/862J-DEVS (revealing that consular officers may google a visa applicant to assess consistency between discoverable facts and those set forth in the application). “For example, a foreign job applicant who prematurely lists a future U.S. employer on a LinkedIn profile may find the visa application delayed while an investigation ensues to ascertain whether he has worked without authorization.” Id.
16 See Social Media Monitoring in US Immigration Process, SIMPLE CITIZEN (Jan. 15, 2020), archived at https://perma.cc/EN6F-D3WB (noting that the DHS began asking immigrants and visitors to share their social media information through four pilot screening programs put in place by the Obama administration); Ron Nixon, U.S. to Collect Social Media Data on All Immigrants Entering Country, N.Y. TIMES (Sept. 28, 2017), archived at https://perma.cc/BS9V-4VFJ (disclosing that it was during the Obama administration that the DHS began asking visitors to voluntarily provide social media information); Walter Ewing, DHS Wants to Monitor Immigrants’ Social Media. No One Knows What They Will Do With This Information, YUBANET.COM (Oct. 2, 2017), archived at https://perma.cc/2ZGU-A4V4 (mentioning that the Obama administration made a few forays into the monitoring of social media via voluntary pilot programs among particular groups of visitors to the U.S.); Aliya Sternstein, Obama Team Did Some ‘Extreme Vetting’ of Muslims Before Trump, New Documents Show, DAILY BEAST (Jan. 2, 2018), archived at https://perma.cc/72CS-5EAA (finding that five months before President Trump came to office, the Obama administration added social media checks to a program that scrutinizes persons from majority-Muslim nations).
media messages of foreign nationals applying for U.S. visas.\textsuperscript{17} Despite pressure from DHS and USCIS officials to allow for the review of visa applicants’ publicly-posted social media messages, the Obama administration upheld the ban, citing their concern of violating individual privacy and fear of bad public relations.\textsuperscript{18} This decision was met with backlash from many DHS and government officials, who contended that the administrations’ arguments were made in bad faith and the government should use every resource available to fully vet foreign nationals seeking entry into the U.S.\textsuperscript{19} In late 2014, the DHS

\textsuperscript{17}See Brian Ross et al., Secret US Policy Blocks Agents From Looking at Social Media of Visa Applicants, Former Official Says, ABC News (Dec. 14, 2015), archived at https://perma.cc/45KQ-VY78 (referencing the secret U.S. policy that prohibited the review of social media messages of foreign nationals). John Cohen, former DHS acting under-secretary for intelligence and analysis, explained that “immigration officials were not allowed to use or review social media as part of the screening process.” \textit{Id.}

\textsuperscript{18}See id. (mentioning that John Cohen and others pressed hard for a policy change and the issue reached a head at a heated 2014 meeting involving Homeland Security Deputy Secretary and other top deputies and representatives of the DHS Office of Civil Liberties and the Office of Privacy). “Immigration, security, law enforcement officials recognized at the time that it was important to more extensively review public social media postings because they offered potential insights into whether somebody was an extremist or potentially connected to a terrorist organization or a supporter of the movement.” \textit{Id.} However, the government’s concern is that social media reviewing would be viewed negatively if it was disclosed publicly and lead to civil liberties backlash. \textit{Id.} See also Fox News, Secret US policy blocks agents from viewing social media of visa applicants, N.Y. POST (Dec. 14, 2015), archived at https://perma.cc/H535-DURK (explaining that Homeland Security Secretary Jeh Johnson refused in early 2014 to end the secret U.S. policy, even though several other officials pressed for such a policy change). See also Seung Min Kim, DHS chief: ‘Legal limits’ on scrutinizing immigrants’ Web postings, POLITICO (Dec. 15, 2015), archived at https://perma.cc/S76U-6QNG (explaining that there are legal limits that restrict federal officials from scrutinizing the social media histories of foreigner nationals). Jeh Johnson emphasized that social media deals with private communications and things for which there is an expectation of privacy, and as such, there are certain legal constraints on government intrusion. \textit{Id.}

\textsuperscript{19}See Fox News, supra note 18 (mentioning government officials’ disappointment that the senior leadership would not approve a review of what were publicly posted online messages). “There is no excuse for not using every resource at [the government’s] disposal to fully vet individuals before they come to the United States.” \textit{Id.} See also SEN. CRUZ TO SECRETARY JOHNSON: DHS POLICY RESTRICTING USE OF SOCIAL MEDIA FOR INVESTIGATIVE PURPOSES IS EXCEEDINGLY DANGEROUS, TED CRUZ (Jan. 22, 2016), archived at https://perma.cc/XDP4-D3QY (expressing U.S. Senator Ted Cruz’s condemnation
loosened these policy restrictions and began pilot programs to include social media in vetting foreign nationals, but even so, social media checks were very rarely used.\textsuperscript{20}

Calls for social media vetting greatly intensified in late 2015, following the shootings in San Bernardino, California by Tashfeen Malik (“Malik”), who entered the U.S. on a K-1 or ‘fiancée’ visa.\textsuperscript{21} Despite her various social media posts pledging allegiance to the Islamic State and supporting jihad and martyrdom, Malik’s multiple immigration background checks failed to uncover her extremist views, of DHS’s negligent blindness to publicly available information on social media). The DHS’s policy is blind to information made available on social media and the internet and restricts fraud and terrorism investigators from fulfilling their missions, thus arguably enabling fraudulent and dangerous people to enter and remain in the U.S. \textit{Id.}

\textsuperscript{20} See Don Reisinger, \textit{Homeland Security Increases Use of Facebook to Identify Terrorists}, FORTUNE (Dec. 15, 2015), archived at https://perma.cc/8LQD-UWP5 (explaining that the DHS policy changed in late-2014, but social media checks were still few and far between). \textit{See also} Ross et al., \textit{supra} note 17 (revealing that current officials said the DHS social media pilot programs were not widespread); Timeline of Social Media Monitoring for Vetting by the Department of Homeland Security and the State Department, BRENNAN CTR. JUST. (May 21, 2021) [hereinafter Timeline], archived at https://perma.cc/HM9Q-LEMF (mentioning that social media monitoring began as nothing more than a small cadre of officers manually checking certain applicants’ social media accounts).

\textsuperscript{21} See Associated Press, \textit{Mother of shooter in San Bernardino terrorist attack sentenced for shredding planning document}, KTLA (Feb. 11, 2021), archived at https://perma.cc/2A2Y-2YJF (explaining that on December 2, 2015, Tashfeen Malik and her husband opened fire during a holiday party and training session, killing 14 people and wounding 22); SEN. CRUZ TO SECRETARY JOHNSON: DHS POLICY RESTRICTING USE OF SOCIAL MEDIA FOR INVESTIGATIVE PURPOSES IS EXCEEDINGLY DANGEROUS, \textit{supra} note 19 (arguing that DHS’s policy of willful blindness toward the reality and danger of radical Islam in the U.S. contributed to the death of 14 Americans in the U.S.). \textit{See also} The K-1 Visa, Explained, BOUNDLESS (Oct. 17, 2021), archived at https://perma.cc/82JP-KMWG (providing details on the K-1 visa). “A K-1 visa – also called a fiancée visa – allows the engaged partner of a U.S. citizen to enter the U.S., as long as the couple gets married no more than 90 days later. The newly married spouse can then apply for permanent residence (a ‘green card’) based on marriage.” \textit{Id.} \textit{See also} Tal Kopan, US to require would-be immigrants to turn over social media handles, CNN (Mar. 29, 2018), archived at https://perma.cc/3CML-587J (highlighting that after the San Bernardino terrorist attack in 2015, greater attention was placed on immigrants’ social media use).
and she was granted her visa in May 2014.\textsuperscript{22} In response to the shooting, lawmakers and members of Congress demanded that the U.S. increase and expand social media monitoring to vet foreign nationals before they are admitted into the U.S.\textsuperscript{23} In 2015, USCIS began new pilot programs to expand social media surveillance through the use of both manual and automated screening.\textsuperscript{24} These pilot

\textsuperscript{22} See Reisinger, supra note 20 (explaining that Malik used social networks to voice her support for jihad before applying for a U.S. visa, but despite those postings, her visa application was approved); ACLJ.org, Obama Admin Must Review Social Media Posts in Vetting, ACLJ (Dec. 15, 2015), archived at https://perma.cc/52JC-7FAL (describing Malik as a radical Islamic jihadist who posted numerous social media messages about violent jihad and said she supported it and wanted to be a part of it); Matt Apuzzo, Michael S. Schmidt & Julia Preston, U.S. Visa Process Missed San Bernardino Wife’s Online Zealotry, N.Y. TIMES (Dec. 12, 2015), archived at https://perma.cc/TQ4G-K99E (explaining that Malik passed three background checks by American immigration officials but none uncovered what she had said online about her views on violent jihad).

\textsuperscript{23} See Ross et al., supra note 17 (mentioning that Senator Charles Schumer, D-N.Y., demanded that the U.S. immediately initiate a program that would check the social media sites of those admitted on visas). “Had they checked out Tashfeen Malik,” the senator said, “maybe those people in San Bernardino would be alive.” Id. See also Off. of Inspector Gen., OIG, DHS Pla

\textsuperscript{24} See Nixon, supra note 16 (stating that “[d]uring the Obama administration, the DHS began asking visitors to voluntarily provide social media information, and had four pilot screening programs”); Brandi Vincent, DHS Plans to Expand Social Media Collection on Refugees and Immigrants, NEXTGOV (Sept. 5, 2019), archived at https://perma.cc/2UKD-3Q7Z (explaining that under the Obama administration, the DHS added a voluntary question regarding social media in the Electronic System for Travel Authorization form, which is the visa waiver program used by travelers from Europe, the United Kingdom and Australia to enter the U.S); Edward Hasbrouck, Obama Admin’s parting gift to foreign visitors: social media surveillance, PAPERS, PLEASE! (Dec. 25, 2016), archived at https://perma.cc/F7H6-6EGF (providing that as part of the online Electronic System for Travel Authorization, tourists, business travelers, and foreign citizens visiting friends and relatives in the U.S. are now being asked to disclose their social media usernames and IDs). \textit{See also DHS Inspector General Report, supra note 23, at 1 (explaining that DHS established a task force to review the Department’s current use of social media and identify options to optimize its use across DHS). According to the Government Accountability Office, “[t]he pilot phase allows for a check on whether program operations occur as expected” but that the pilot programs should have well-defined, clear, and measurable objectives. Id. at 2. \textit{See also Timeline, supra note 20 (stating that in December 2015, DHS began
programs aimed to examine the feasibility of social media screening and to determine whether useful information could be obtained for adjudicating refugee applications.  

2. The Trump Administration

While the Obama administration set the groundwork for USCIS to begin collecting social media data, the Trump administration greatly expanded these practices through its “extreme vetting” program and the implementation of numerous new policies.  

both manual and automatic screening of the social media accounts of a limited number of individuals applying to travel to the U.S., through various non-public pilot programs).

25 See DHS Inspector General Report, supra note 23, at 1 (noting that the DHS task force’s “first priority was to conduct a pilot program at USCIS to test systematic screening of applicants for immigration benefits.”). The pilot program aimed to examine the feasibility of using social media screening with an [unnamed] automated search tool. Id. at 2. The task force ultimately intended to use the pilot program and lessons learned from other DHS components’ use of social media to develop policies and processes for standardized use of social media department wide. Id. at 1. See also Ross et al., supra note 17 (communicating that the DHS “will continue to ensure that any use of social media in its vetting program is consistent with current law and appropriately takes into account civil rights and civil liberties and privacy protections”).

26 See Nixon, supra note 16 (admitting that even though the Obama administration collected social media information, the new monitoring put in place by the Trump administration represented an escalation). See also Exec. Ord. 13780, supra note 6, at 13209 (describing Trump’s aim to improve the screening and vetting protocols and procedures associated with the visa-issuance process and the United States Refugee Admissions Program). See also Faiza Patel, Trump’s Latest Half-Baked Muslim Ban, DAILY BEAST (June 13, 2017), archived at https://perma.cc/5VFH-6VXH (explaining the similarity between Trump’s Muslim ban and extreme vetting). Trump introduced extreme vetting in a campaign speech, as part of his plan for stopping immigration from Syria and Libya, but also emphasized that “[w]e’re going to have extreme vetting in all cases. And I mean extreme.” Id. See Stop Collecting Immigrants’ Social Media Data, supra note 5 (explaining that when Trump’s Muslim “ban was struck down by federal courts, the State Department imposed additional vetting measures that just happened to cover about the same number of people as the ban.”). See also Harsha Panduranga, The ‘Muslim Ban’ Is Gone. Now What?, BRENNAH CTR. JUST. (Jan. 21, 2021), archived at
limited information on the effectiveness of DHS’s 2015 pilot programs, in May 2017, the State Department issued an emergency notice, requesting that visa applicants who had been determined to warrant additional scrutiny be required to provide their social media user identifiers (also known as usernames or “handles”) used during the last five years from the date of the application. Moreover, in September 2017, the DHS issued a Notice to the public indicating that social media handles, aliases, associated identifiable information, and search results would be stored in updated A-file records for noncitizens and lawful permanent residents, as well as naturalized or foreign-born citizens of the U.S.

This new social media collection and retention https://perma.cc/YFD4-RWXR (arguing that “Trump campaign officials signaled years ago that expanded social media screening was to be the Muslim ban’s digital complement to restrict entry to only those who have government-approved views and beliefs.”).

See DHS Inspector General Report, supra note 23, at 2 (disclosing that DHS’s pilot programs lack criteria for measuring performance to ensure they meet their objectives). Because it is not clear DHS is measuring and evaluating the pilots’ results to determine how well they are performing, the pilots will be of limited use in planning and implementing an effective, department-wide future social media screening program. Id. See also Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 20956, 20957 (2017) [hereinafter 2017 Notice] (explaining that the State Department will use Form DS-5535 to collect social media platforms and identifiers used during the last five years from “immigrant and nonimmigrant visa applicants who have been determined to warrant additional scrutiny in connection with terrorism or other national security-related visa ineligibilities.”). “The collection of social media platforms and identifiers will not be used to deny visas based on applicants’ race, religion, ethnicity, national origin, political views, gender, or sexual orientation.” Id. But see Timeline, supra note 20 (describing comments submitted by civil and human rights organizations arguing that the State Department proposal is excessively burdensome and vague, is apt to chill speech, is discriminatory against Muslims, and has no security benefit). See also Social Media Surveillance, ASIAN AMS. ADVANCING JUST., (Jan. 16, 2022), archived at https://perma.cc/6P5S-D9CR (arguing that the State Department’s policy proposal targets individuals from predominantly Muslim countries impacted by President Trump’s travel ban).

See 2017 Privacy Act, supra note 4, at 43559 (listing the categories of individuals covered by the policy, including lawful permanent residents, naturalized U.S. citizens, individuals petitioning for Immigration and Nationality Act (“INA”) benefits, legal guardians of immigrants with a physical or mental disability, and other persons subject to the vast provisions of the INA); Hu, supra note 4, at 1274 (emphasizing that the DHS policy allows for social media data to be retained in the A-Files for both noncitizens and lawful permanent residents, as well as naturalized or foreign-born citizens of the U.S.). See also Nixon, supra note 16 (providing that
policy led to an outcry of criticism from privacy groups and members of the public, arguing that the policy lacked sufficient information, was burdensome to legal immigration, and threatened individuals’ rights to free speech and privacy.\textsuperscript{29} Notably, a coalition of twenty-seven organizations argued that the social media collection policy could be broadly interpreted to encompass the gamut of someone’s online activity, which could cause individuals to self-censor, delete their social media accounts, and disengage from online spaces.\textsuperscript{30}

the department will begin collecting social media information on October 18, 2017, the same day the Trump administration’s new travel ban on citizens of seven countries and restrictions on those from two others are set to take effect); Sewell Chan, \textit{14 Million Visitors to U.S. Face Social Media Screening}, \textit{N.Y. TIMES} (Mar. 30, 2018), \textit{archived at} https://perma.cc/VT9R-3MAG (finding that the Trump administration’s policy would affect 710,000 people or so a year).

\textsuperscript{29} See Thomas Campbell, \textit{Full Transparency: A Case Against the Collection of Internet Information in Trump-Era American Immigration}, 13 FIU L. REV. 513, 514 (2019) (highlighting that during the customary 30-day comment period before the policy went into effect, 2,994 public comments were submitted, the vast majority of which offered scathing critiques of the new DHS policy). U.S. Representative Ted Lieu, a naturalized U.S. citizen, expressed his concern that the policy would apply to U.S. citizens like himself, as well as argued that the Notice contained ambiguous provisions and needed clarification. \textit{Id.} at 515. \textit{See also} Hu, \textit{supra} note 4, at 1280–84 (emphasizing that the DHS policy was highly controversial and resulted in comments focusing on constitutional law concerns, privacy act and administrative law concerns, and data collection, storage, and use concerns); Kopan, \textit{supra} note 21 (noting critics’ complaints that the policy, amid broader efforts by the administration, is not only invasive on privacy grounds, but also effectively limits legal immigration to the U.S. by slowing the process down, making it more burdensome and making it more difficult to be accepted for a visa); Nixon, \textit{supra} note 16 (quoting Faiz Shakir, the national political director for the American Civil Liberties Union, that the policy “would undoubtedly have a chilling effect on the free speech that’s expressed every day on social media”).

\textsuperscript{30} See Timeline, \textit{supra} note 20 (noting that on October 18, 2017, a coalition submitted comments expressing opposition to DHS social media retention). \textit{See also Coalition Letter Opposing DHS Social Media Retention, HUM. RTS. WATCH} (Oct. 18, 2017), \textit{archived at} https://perma.cc/P3JD-64KL (arguing that the DHS’s notice raises concerns that the collection, retention, use, and sharing of social media information will invade the privacy of immigrants and U.S. citizens, chill freedom of speech and association, invite abuse in exchange for little security benefit, and establish a system that treats naturalized citizens as second-class citizens). The policy’s failure to define the term “social media” allows it to include not only Twitter and Facebook,
Nevertheless, the Trump administration and DHS both defended and sought to further enhance their social media monitoring policy.\(^{31}\) Within the next year, the State Department expanded this social media collection policy to apply to both immigrant and nonimmigrant visas – greatly increasing the number of foreign nationals required to provide social media identifiers.\(^{32}\) Under these new policy proposals, applicants would be required to provide social media user identifiers for various social media platforms used by the applicant during the past five years on mandatory immigration forms.\(^{33}\)

but also platforms that might reveal professional networks, romantic interests, news and entertainment consumption, and a wide range of other particularly sensitive information. \(^{31}\) Public social media can reveal more and different information than people may realize or intend to convey, especially as privacy settings are not always fully understood or utilized and may be changed by the platform without notice to the user. \(^{32}\)

\(^{31}\) See Chan, supra note 28 (revealing how DHS Secretary John Kelly told Congress that the DHS was considering asking visitors for passwords and access to online accounts). “We want to get on their social media, with passwords… [i]f they don’t want to cooperate, then you don’t come in.” \(^{32}\) See also Campbell, supra note 29, at 515 (providing that in the wake of public outcry, a spokesperson at the DHS explained that the Notice is not new policy but is simply an effort by the DHS to be more transparent). But see Hu, supra note 4, at 1274 (explaining that the Notice also indicates that social media screening is emerging as a routinized aspect of DHS screening and vetting procedures and is increasingly becoming bureaucratized – treated not as a surveillance practice, but as a records collection practice).

\(^{32}\) See What is the difference between an immigrant visa and nonimmigrant visa?, CITIZENPATH (Oct. 22, 2021), archived at https://perma.cc/F433-7XZT (explaining that the U.S. grants an immigrant visa to foreign-born individuals who intend to make the U.S. a permanent home, and issues a nonimmigrant visa to people who are temporarily visiting the U.S. for tourism, medical treatment, temporary work, school and other reasons). See also Timeline, supra note 20 (noting that in March 2018, the State Department issued notices of proposals to collect a range of information from applicants for both immigrant and non-immigrant visas). “The proposal seeks to ask all visa applicants – an estimated 14.7 million people per year – to provide social media identifiers, telephone numbers, and email addresses used in the past five years, among other information.” \(^{33}\) See Chan, supra note 28 (explaining that the new proposal would add a tangible new requirement for millions of people who apply to visit the U.S. for business or pleasure, including citizens Brazil, China, India and Mexico). Citizens of roughly 40 countries to which the U.S. ordinarily grants visa-free travel, including major allies like Australia, Britain, Canada, France, Germany, Japan, and South Korea, will not be affected by the requirement. \(^{33}\)

\(^{33}\) See U.S. Dep’t. of State, 60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration, 83 Fed. Reg. 13806, 13806 (Mar. 30, 2018) (indicating that the DHS is revising the Electronic Application for
Finally, in September 2019, in an attempt to expand the policy even further, the DHS issued a proposal to collect social media data from Visa Waiver Program applicants and applicants seeking immigration benefits, including adjustment of status, naturalization, and asylum status. 34
C. The Impact of Social Media Monitoring Policies

1. Lack of Proven Effectiveness

The DHS argues that the collection of foreign nationals’ social media data is necessary to identify national security threats, however, various organizations and individuals have criticized the enacted policies for their lack of proven effectiveness. In addition to outside criticism, research and reports conducted by DHS and USCIS have revealed the ineffectual use of their social media monitoring programs to identify threats. In February 2017, DHS’s Office of Inspector

35 See Lau, supra note 6 (arguing that “while the government has justified its expansion [of social media monitoring programs] in the name of national security, there is little indication that these programs – or the algorithms that sometimes power them – are effective in achieving their stated goals.”); Rachel Levinson-Waldman, Government surveillance of social media related to immigration more extensive than you realize, THE HILL (May 29, 2019), archived at https://perma.cc/YS6D-3KL2 (mentioning that “[t]he breadth of DHS’s social media monitoring begs the question: Is it effective?”); Waheed, supra note 8 (criticizing the Trump administration for moving forward with its social media vetting initiatives despite the absence of any evidence that they can be carried out fairly and effectively). See also Carrie Decell & Harsha Panduranga, Social Media Vetting of Visa Applicants Violates the First Amendment, KNIGHT FIRST AMEND. INST. COLUM. UNIV. (Dec. 6, 2019), archived at https://perma.cc/MD6V-ER9K (stressing that “despite the State Department’s bare assertion that collecting social media information will ‘strengthen’ the processes for ‘vetting applicants and confirming their identity,’ the government has failed—in numerous attempts—to show that social media screening is even effective as a visa-vetting or national security tool.”). See also Hugh Handeyside, ‘Extreme Vetting’ of Visitors Poses an Extreme Threat to Our Principles and Our Security, (Apr. 10, 2017), archived at https://perma.cc/8AGA-Q6JK (arguing that “people with bad intentions will take steps to wipe their devices and conceal any other content that may raise concerns.”). The DHS inspector general even concluded that “there’s no effective way to analyze the massive amounts of data gleaned from social media data dumps.” Id.  

36 See Doc Society v. Blinken, BRENNAN CTR. JUST. (Dec. 5, 2019), archived at https://perma.cc/7NL3-HWB9 (revealing that in 2017, the DHS Inspector General concluded that “the social media screening pilot programs it reviewed failed to measure effectiveness and could not justify scaling the practice.”). In addition, “[o]ther internal DHS reviews pointed out that officials found it difficult to make use of social media data to identify national security threats.” Id. See also DHS Inspector General Report, supra note 23, at 4 (arguing that the DHS task force “needs to better manage ongoing efforts to pilot social media screening to help ensure an effective and successful social media screening program in the future.”). In reviewing one of their pilot programs, USCIS concluded that the [unnamed] tool they
General audited five USCIS programs and concluded that DHS had failed to establish mechanisms to measure the effectiveness of their programs. Specifically, the report indicated that the DHS’s pilot programs “[lacked] criteria for measuring performance to ensure they meet their objectives” and as a result, the pilots provided “limited information for planning and implementing an effective, department-wide future social media screening program.” Moreover, USCIS concluded that social media information was neither helpful nor particularly impactful on the processing of cases. Ultimately, USCIS used to screen foreign national’s social media was not a viable option because of its low “match confidence.” Officers had to manually check the results because the accounts identified by the tool often did not match up with the applicants. See also Stop Collecting Immigrants’ Social Media Data, supra note 5 (stating that “it’s no surprise that the D.H.S.’s own pilot programs show that social media has not been useful in identifying threats.”).

37 See DHS Inspector General Report, supra, note 23, at 2 (revealing that “it is not clear DHS is measuring and evaluating the pilots’ results to determine how well they are performing.”). “Because the pilot did not have metrics to measure success, it is difficult to conclude whether finding [redacted] individuals with confirmed social media accounts constitutes success.” Id. at 3.

38 See id. at 2 (providing the results of the DHS’s inspection of their pilot programs). See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (revealing that the audit of DHS’s social media pilot programs found that “insufficient metrics were in place to measure the programs’ effectiveness, and concluded that existing pilots had provided little value in guiding the rollout of a department-wide social media screening program.”). Documents found that the programs were expensive and time consuming but provided little useful information. Id.

39 See Social Media Monitoring, supra note 7 (presenting findings of USCIS’s own evaluations of its social media monitoring programs). “[O]ut of the 12,000 refugee applicants and 1,500 immigration benefit applicants screened, USCIS found social media information helpful only in ‘a small number of cases,’ where it ‘had a limited impact on the processing of those cases – specifically in developing additional lines of inquiry.’” Of the 1,500 immigration benefits cases reviewed, none were denied “solely or primarily because of information uncovered through social media vetting.” Ultimately, the pilot programs struggled to reliably match social media accounts to the individual being vetted, and even where the correct accounts were found, it was difficult to analyze the data for national security threats. Id. See also Sternstein, supra note 16 (finding that as of November 2016, no immigration benefits had been denied “solely or primarily because of information uncovered through
found that it was hard to determine with any level of certainty the “authenticity, veracity, [or] social context” of a foreign national’s social media data as well as whether the data contained “indicators of fraud, public safety, or national security concern.”

2. The Impact of Social Media Monitoring on Constitutional Rights

a. Infringement on First Amendment Rights

As the DHS expanded its collection of social media information, many critics argued that the widespread monitoring and retention of such data threatened both foreign nationals’ and U.S. citizens’ freedom of speech and association. The First Amendment social media vetting.”). Even in cases of benefit denial, the denial was not based on information found from social media, but on information found through routine security and background checks or uncovered during an interview. Id. See also Harsha Panduranga, White House Office Rejects DHS Proposal to Collect Social Media Data on Travel and Immigration Forms, BRENnan CTR. FOR JUST. (Apr. 27, 2021), archived at https://perma.cc/7RWM-RPD7 [hereinafter Rejection of DHS Proposal] (concluding that “mass social media screening’ was a poor use of resources, taking people away from ‘the more targeted enhanced vetting they are well trained and equipped to do.’”).

40 See Social Media Monitoring, supra note 7 (emphasizing that “[t]he difficulties faced by DHS personnel are hardly surprising [as] attempts at making judgments based on social media are plagued by problems of interpretation.”). In one example of flawed interpretation of social media posts, “a British national was denied entry at a Los Angeles airport when DHS agents misinterpreted his posting on Twitter that he was going to ‘destroy America’ – slang for partying – and ‘dig up Marilyn Monroe’s grave’ – a joking reference to a television show.” Id. See also Stop Collecting Immigrants’ Social Media Data, supra note 5 (explaining that posts and tweets are often unreliable as people posture, joke, speak in shorthand and use cultural references that are hard for others to interpret). In addition, “[a]ccuracy takes a nose-dive when the speech being analyzed is not standard English.” Id. See also Lau, supra note 6 (emphasizing that the DHS pilot programs struggled to interpret what was in the social media messages and connect them to actual threats). Interpretation problems only became even more complex when a non-English language or unfamiliar cultural context was involved. Id.

41 See Rodil, supra note 4, at 270 (stating that the national political director for the ACLU predicted that the policy would “undoubtedly have a chilling effect on the free speech that’s expressed every day on social media.”). In addition, the social media monitoring policies threatened to chill freedom of association, which is a possible First Amendment violation. Id. See also Stop Collecting Immigrants’
of the U.S. Constitution, which applies to both citizens as well as non-citizens legally inside the U.S., prohibits the government from either directly or indirectly abridging the right to free speech in most cases.\textsuperscript{42} For example, in \textit{Reno v. ACLU}, the Supreme Court ruled that a law which made it a crime to engage in online speech that is “indecent” or

\textit{Social Media Data, supra} note 5 (arguing that the centralization of highly personal information in the hands of the DHS threatens freedom of speech and association); \textit{Social Media Monitoring, supra} note 7 (providing that social media monitoring will “impact what people say online, leading to self-censorship of people applying for visas as well as their family members and friends.”).

\textsuperscript{42} See U.S. CONST. amend. I (stating that “Congress shall make no law … abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble …”); Packingham v. North Carolina, 137 S. Ct. 1730, 1731 (2017) (holding that “[a] fundamental First Amendment principle is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more.”). \textit{See also} Miller, \textit{supra} note 2, at 417 (explaining that laws directly forbidding certain types of speech are an obvious violation of the First Amendment, but laws that merely discourage certain types of speech may also violate the First Amendment). \textit{See also} Julia Horowitz, \textit{The First Amendment, Censorship, and Private Companies: What Does “Free Speech” Really Mean?}, CARNEGIE LIBR. PITT. (Mar. 9, 2021), archived at https://perma.cc/6TTW-R59G (explaining that the First Amendment only protects speech from government censorship, which includes federal, state, and local government actors). The First Amendment protections do not apply to private citizens, businesses, and organizations, which means that social media platforms can legally establish regulations and guidelines within their communities. \textit{Id. See also} Eugene Volokh, \textit{First Amendment, BRITANNICA} (Oct. 23, 2021), archived at https://perma.cc/LK4Y-23ES (noting that there are historically rooted exceptions to the First Amendment, including incitement, defamation, fraud, obscenity, child pornography, fighting words, and threats). \textit{See also} Bridges v. Wixon, 326 U.S. 135, 148 (1945) (establishing that the freedom of speech and of press is accorded to aliens residing in the U.S.). “[O]nce an alien lawfully enters and resides in this country he becomes invested with the rights guaranteed by the Constitution to all people within our borders. Such rights include those protected by the First and the Fifth Amendments and by the due process clause of the Fourteenth Amendment.” \textit{Id.} at 161 (Murphy, J., concurring); Kwong Hai Chew v. Colding, 344 U.S. 590, 596 n.5 (1953) (finding that neither the First nor Fifth Amendment distinguishes between citizens and “resident aliens”). \textit{See also} Rodil, \textit{supra} note 4, at 271–72 (explaining that there are Supreme Court cases that have interpreted that Fourteenth and Fifth Amendment protections apply to non-citizens on the basis that the Amendments protect “people” rather than explicitly mentioning citizens). Therefore, a similar logic and application of the word “persons” might be applied in First Amendment cases. \textit{Id.} at 272.
“patently offensive” was unconstitutional because the terms “indecent” and “patently offensive” were vague and overbroad and therefore threatened to cause uncertainty among speakers.43 This indirect infringement of the First Amendment, known as the “chilling effect,” occurs when a law causes individuals or groups to refrain from engaging in speech or expression for fear of running afoul of the law or regulation.44 Typically, the chilling effect occurs when a law is either too broad or too vague.45

The First Amendment of the U.S. Constitution also includes the freedom of association which protects “expressive” or “intimate” associations from direct or indirect government interference.46

43 See Reno v. Am. C.L. Union, 521 U.S. 844, 845 (1997) (holding that the provision of the Communications Decency Act (CDA) that criminalized the online transmission of “patently offensive” and “indecent” communications raised special First Amendment concerns because of its obvious chilling effect on free speech). The terms “patently offensive” and “indecent” are inherently vague and as a result, the CDA provision “sweeps more broadly than necessary and thereby chills the expression of adults.” Id. at 862. The provision’s use of the undefined terms “indecent” and “patently offensive” will “provoke uncertainty among speakers about how the two standards relate to each other and just what they mean.” Id. at 871.

44 See id. (mentioning that a governmental regulation that unjustly deters some sort of activity which is normally protected by the Constitution can have a chilling effect). See also David L. Hudson, Jr., Chilling Effect Overview, FIRE (Feb. 15, 2017), archived at https://perma.cc/SB92-8K6K (explaining that the chilling effect causes individuals to “steer far clear from the reaches of a law for fear of retaliation, prosecution, or punitive governmental action.”). See also Wieman v. Updegraff, 344 U.S. 183, 195 (1952) (Frankfurter, J., concurring) (referencing the chilling effect of speech for the first time as a “chill” upon freedom of thought and expression).

45 See Hudson, supra note 44 (describing the types of laws that typically cause a chilling effect). Vague laws produce chilling effects because individuals do not know exactly when their expressive conduct or speech crosses the line and violates such rules. Id. Overbroad laws and laws that impose a prior restraint on expression also can chill expression. Id. See also Walker v. City of Birmingham, 388 U.S. 307, 345 (1967) (Brennan, J., dissenting) (referencing the Court’s “overriding duty to insulate all individuals from the ‘chilling effect’ upon exercise of First Amendment freedoms generated by vagueness, overbreadth and unbridled discretion to limit their exercise.”).

46 See Jonathan Sabin, Every Click You Make: How the Proposed Disclosure of Law Students' Online Identities Violates Their First Amendment Right to Free Association, 17 J. L. & Pol'y 699, 714 (2009) (explaining that although “freedom of association” is not explicitly mentioned in the Constitution, the Supreme Court has found such a freedom inherent in the First Amendment's protection of free speech and free assembly). The right to free association can be both indirectly infringed, or “chilled,” by government regulation, as well as directly infringed by government
Indirect infringements, or the “chilling” of the right to free association by government regulation, are generally prohibited and will only be upheld if substantially related to compelling state interests. For example, in *NAACP v. Alabama*, the Court found that the mandatory disclosure of National Association for the Advancement of Colored regulations prohibiting organizations from excluding certain individuals. *Id.* at 715. See also *Roberts v. U.S. Jaycees*, 468 U.S. 609, 617–18 (1984) (noting that the Supreme Court has referred to constitutionally protected freedom of association in two distinct senses: associations that are “intimate” and those that are “expressive”). Expressive associations are often for the purpose of engaging in activities that are protected by the First Amendment, including speech, assembly, petition for the redress of grievances, and the exercise of religion. *Id.* at 618. On the other hand, intimate associations “involve deep attachments and commitments to the necessarily few other individuals with whom one shares not only a special community of thoughts, experiences, and beliefs but also distinctively personal aspects of one's life.” *Id.* at 619–20. See also David L. Hudson Jr., *Freedom of Association*, THE FIRST AMEND. ENCYCLOPEDIA (Nov. 14, 2021), archived at https://perma.cc/LG9X-PGZ3 (noting that the right to expressive association is often for political purposes while intimate associations include the right to marriage, the rearing of children, and the right to live with relatives). See also *Boy Scouts of Am. v. Dale*, 530 U.S. 640, 648 (2000) (emphasizing that the First Amendment's protection of expressive association is reserved for any group that engages in some form of expression, whether it be public or private). On the other hand, to be considered intimate, an association must be sufficiently personal or private. *Id.* at 646.

47 See Sabin, supra note 46, at 716 (stating that most indirect infringements on associational freedoms have occurred through state attempts to compel disclosure of organizations' membership lists). Ultimately, state actions such as mandatory disclosure of membership lists that indirectly “chill” free association violate the First Amendment unless substantially related to compelling state interests. *Id.* at 718. A compelling state interest must be unrelated to the suppression of ideas and unable to be achieved through a means significantly less restrictive of associational freedoms. *Id.* at 715. See also Ronald Steiner, *Compelling State Interest*, FIRST AMEND. ENCYCLOPEDIA (Sept. 20, 2022), archived at https://perma.cc/7GEQ-DCZM (providing examples of compelling governmental interests, such as regulation vital to the protection of public health and safety, regulation of violent crime, and requirements of national security and military necessity). See also *Let the End Be Legitimate: Questioning the Value of Heightened Scrutiny's Compelling- and Important-Interest Inquiries*, 129 HARV. L. REV. 1406, 1410 (2016) (explaining that the Court has relied on traditional notions about the proper functions and operation of the state to support its determination that an interest is compelling). For example, the Court has found that a state’s interest in preventing quid pro quo corruption or its appearance and combating terrorism are compelling interests. *Id.* at 1410–11.
People (“NAACP”) membership lists violated the freedom of association because Alabama did not demonstrate a substantial interest in obtaining the disclosures.48 Similarly, in Gibson v. Fla. Legislative Investigation Comm., the Supreme Court overturned Florida’s mandatory disclosure of NAACP membership to investigate Communist activities and identify Communist leaders, arguing that while the state may have had a compelling interest in uncovering members of the Communist Party, the disclosure requirement was not substantially related to that interest.49

In a recently filed and ongoing lawsuit, the Knight Institute, the Brennan Center for Justice, and the law firm Simpson Thacher & Bartlett are challenging the DHS’s social media collection policies on the grounds that the registration requirement violates the First Amendment.50 Specifically, the parties assert that the DHS’s dragnet

---

48 See Nat’l Ass’n for Advancement of Colored People v. Alabama ex rel. Patterson, 357 U.S. 449, 464 (1958) (striking down the mandatory disclosure of membership lists because it did not have a “substantial bearing” on a substantial state interest). “Whatever interest the State may have in obtaining names of ordinary members has not been shown to be sufficient to overcome petitioner’s constitutional objections to the production order.” Id. at 465. See also Sabin, supra note 46, at 716 (explaining that the mandatory disclosure of NAACP membership lists violated the First Amendment because the privacy of group membership was “so related to the rights of the [NAACP] members to…associate freely with others.”). The Court ultimately found that the disclosure requirement did not have a substantial bearing on a substantial state interest, and therefore struck down the disclosure requirement. Id. 49 See Gibson v. Fla. Legisl. Investigation Comm., 372 U.S. 539, 551 (1963) (arguing that Florida did not prove that there was a “substantial connection” between the Miami NAACP and Communist Party activities). “[T]he Committee has not ‘demonstrated so cogent an interest in obtaining and making public’ the membership information sought to be obtained as to ‘justify the substantial abridgment of associational freedom which such disclosures will effect.’” Id. at 546. “Where there is a significant encroachment upon personal liberty, the State may prevail only upon showing a subordinating interest which is compelling.” Id. See also Sabin, supra note 46, at 717 n.120 (presuming that if there was evidence of Communist activity by NAACP members, infringement of their associational freedoms would not be unconstitutional).

50 See Doc Society v. Blinken, supra note 36 (explaining that in December 2019, the Brennan Center, Knight First Amendment Institute at Columbia University, and Simpson Thacher & Bartlett LLP filed the lawsuit on behalf of two U.S. based organizations that collaborate with filmmakers around the world). The lawsuit alleges that the registration requirement and related retention and dissemination policies violate the First Amendment because they chill constitutionally protected speech and association, while being poorly tailored to the government’s stated
collection and retention of social media identifiers over the past five years from nearly all U.S. visa applicants has a dramatic chilling effect on the constitutionally protected speech and association of millions of people around the world.\(^5\)

b. Impact on Privacy and the Fourth Amendment

Along with freedom of speech and association concerns, critics have also argued that social media monitoring poses serious threats to privacy.\(^5\) An individual’s right to privacy stems from the Fourth Amendment of the U.S. Constitution, which has been held to apply to non-citizens legally inside the U.S.\(^5\) The right to privacy under the

---

interests. Id. See also Glenn, supra note 10 (explaining that the Trump-era government policy providing for the mass collection and indefinite retention of visa applicants’ social media identifiers is at the heart of a First Amendment lawsuit).

\(^5\) See Glenn, supra note 10 (arguing that “the registration requirement deters people who decide to apply for U.S. visas from freely sharing their views and engaging with others on social media, for fear that their speech will be misinterpreted or used against them.”). In particular, visa applicants who use pseudonyms on social media to protect themselves from retaliation or reprisal by government or private actors are especially burdened by the registration requirement. Id. Ultimately the expansive nature of the DHS’s social media registration requirement and the data that the government is collecting is out of balance with the First Amendment rights at stake. Id. See also Doc Society v. Blinken, supra note 36 (emphasizing that the DHS policies that contemplate the retention of applicants’ social media data and permit using it for broadly defined purposes magnify First Amendment chilling effects).

\(^5\) See Social Media Monitoring, supra note 7 (arguing that social media monitoring creates serious risks to privacy and free speech). “The deleterious effect of surveillance on free speech has been well documented in empirical research; one recent study found that awareness or fear of government surveillance of the internet had a substantial chilling effect among both U.S. Muslims and broader U.S. samples of internet users.” Id. See also Miller, supra note 2, at 411 (holding that the DHS collecting and storing social media handles raises privacy concerns under the Fourth Amendment); Handeyside, supra note 35 (noting that vetting measures would be equally damaging to privacy and online security, for Americans and foreigners alike).

\(^5\) See U.S. Const. amend. IV (identifying the basis of an individual’s right to privacy). The Fourth Amendment states:
Fourth Amendment exists in instances where an individual exhibits a subjective expectation of privacy and society recognizes that expectation of privacy as reasonable.\textsuperscript{54} However, the Supreme Court has held that individuals do not have a reasonable expectation of privacy when they knowingly give their private information to a third party.\textsuperscript{55} This concept, known as the third-party doctrine, was solidified

\textit{The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.}

\textit{Id. See also} Mapp v. Ohio, 367 U.S. 643, 650 (1961) (declaring that the “security of one’s privacy against arbitrary intrusion by the police’ is ‘implicit in ‘the concept of ordered liberty.’”). The Fourth Amendment’s right of privacy has been declared enforceable against the States through the Due Process Clause of the Fourteenth Amendment and by the same sanction of exclusion as is used against the Federal Government. \textit{Id. at 655. See also Miller, supra note 2, at 401 (explaining that noncitizens, once inside the U.S., share many of the same protections guaranteed by the Constitution as citizens, including those of the Fourth Amendment). See also Marisa Antos-Fallon, The Fourth Amendment and Immigration Enforcement in the Home: Can ICE Target the Utmost Sphere of Privacy?, 35 \textit{Fordham Urb. L.J.} 999, 1015 (2008) (arguing that courts have repeatedly recognized that the language of the Fourth Amendment extends to non-citizens). Courts consider the privacy interests of legal immigrants and citizens when evaluating the constitutionality of immigration enforcement, regardless of the immigration status of the person or persons that are the target of the operation. \textit{Id.}

\textsuperscript{54} See \textit{Katz v. United States}, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (outlining the two-prong analysis for the right to privacy). First, a person must exhibit an actual (subjective) expectation of privacy and, second, that the expectation must be one that society is prepared to recognize as reasonable. \textit{Id.} For example, an individual has a constitutionally protected reasonable expectation of privacy within an enclosed telephone booth. \textit{Id. at 360.} One who occupies a telephone booth shuts the door behind him and assumes that his conversation is not being intercepted, and such expectations of privacy are recognized as reasonable. \textit{Id. at 360–61. But see} California v. Greenwood, 486 U.S. 35, 40–41 (1988) (holding that a person who deposits their garbage “in an area particularly suited for public inspection” doesn’t have a reasonable expectation of privacy for trash left in a publicly accessible place). An individual puts their trash at the curb for the express purpose of conveying it to a third party, the trash collector, and it is common knowledge that plastic garbage bags left on a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. \textit{Id. at 40.}

\textsuperscript{55} See \textit{Smith v. Maryland}, 442 U.S. 735, 743–44 (1979) (emphasizing that the Supreme Court has consistently held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties). See also Brian
by the Supreme Court in *Smith v. Maryland*, in which the Court held that an individual does not have a Fourth Amendment interest in the phone numbers they dial, since these numbers are passed on to the telephone company. The third-party doctrine similarly applies to social media information and establishes that individuals do not have a reasonable expectation of privacy in social media data.

Mund, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J. L. & TECH. 238, 242–243 (2017) (revealing that individuals “do not have a reasonable expectation of privacy against government searches or intelligence-gathering efforts that occur in public settings or where citizens expose private information to a third party.”); Miller, *supra* note 2, at 414 (explaining that when an individual reveals information to a third-party, that individual has assumed the risk of the shared information not remaining private, and therefore the reasonable expectation of privacy test does not apply).

See *Smith*, 442 U.S. at 745–46 (holding that the installation and use of a pen register did not violate the defendant’s expectation of privacy because dialed phone numbers are turned over to third parties). When petitioner voluntarily exposed numerical information to the phone company, he assumed the risk that the company would reveal the information to the police. *Id.* at 744. Even if defendant did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society recognizes as reasonable because a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. *Id.* at 743–44.

See Mund, *supra* note 55, at 243 (describing the third-party doctrine which “severely cabins Fourth Amendment protections by creating an exception to the reasonable expectation of privacy.”). As soon as one posts information on a social media platform, the poster discloses information to the third-party platform operator, and, for most social networking posts, to all of the members within the poster’s social network. *Id.* at 244. See also Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 2 (2013) (explaining that majority of communications over the Internet, such as Facebook messages and emails, are stored on third party servers or Internet service providers known as ISPs). “Because Internet communications are… voluntarily disclosed to machines in the form of ISPs, arguably under *Smith* users appear to lose any Fourth Amendment protection in these communications.” *Id.* at 3. The government could therefore obtain these online communications from the third-party service provider and use the information against a person at trial without needing to first obtain a warrant. *Id.* See also Renee M. Jackson, *No reasonable expectation of privacy in content posted to social networking websites, regardless of individual privacy settings*, NIXON PEABODY LLP (Oct. 13, 2010), archived at https://perma.cc/Z5UG-FKN9 (highlighting that a trial court found that regardless of the privacy settings
Although the Supreme Court has tried to restrict the rein of the third-party doctrine in specific instances, many scholars argue that in our current digital age, the third-party doctrine as a whole should be reconsidered. Specifically, they argue that the third-party doctrine was established long before the existence of the internet and social media, and is ill-suited for our current society in which people constantly reveal a great deal of information about themselves to third parties during the course of their everyday life. Through information collected on various social media platforms alone, the government has been given the ability to liberally glean the most intimate details about

used to restrict access to social media postings, an individual has no reasonable expectation of privacy in what they post to their Facebook or social media accounts). See Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that location data does not fall under the third-party doctrine). “Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection… an individual maintains a legitimate expectation of privacy in the record of his physical movements.” Id. See also Campbell, supra note 29, at 531 (revealing that many scholars recognize the inherent problems associated with the third-party doctrine). “The Fourth Amendment has been stretched in favor of the U.S. government, under the guise of national security.” Id. The only way to rectify the mishap that is the third-party doctrine is to bring a case to the Supreme Court to potentially rescind the doctrine. Id. at 532. Through this course of action, citizens and certain noncitizens alike could have their Fourth Amendment privacy protections restored. Id. See Campbell, supra note 29, at 532 (arguing that “the third-party doctrine is an outdated jurisprudential mishap.”). See also United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (stating that it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties).

This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

Id. All information voluntarily disclosed to some member of the public for a limited purpose should not be disentitled to Fourth Amendment protection. Id. at 418. See also Harvey Gee, Last Call for the Third-Party Doctrine in the Digital Age After Carpenter?, B.U. J. SCI. & TECH. L. 286, 288 (2020) (characterizing the third-party doctrine as “anachronistic” in the current age of surveillance). The types of limited personal information at issue in Smith, such as 1970s era bank records and landline phone records, cannot be compared to the exhaustive amount of communicative content casually collected by wireless carriers and social media platforms today. Id. at 289.
an individual from content such as private messages, documents and photos, search queries and browsing history, fitness/health activity, and romantic involvement.  

III. Facts

A. The Biden Administration – Where we are Now

President Biden has adopted a series of immigration executive orders and revoked many of former President Trump’s immigration policies and programs, but nevertheless, his administration has failed to fully rescind the practice of collecting and retaining foreign nationals' social media identifiers.61 As part of the same proclamation in which he rescinded former President Trump’s Muslim and African Bans and “extreme vetting” practices, President Biden directed the State Department, DHS, and the Director of National Intelligence to review the current use and effectiveness of social media identifiers for

60 See Gee, supra note 59 at 288 (stating that “[i]t is unreasonable to argue that by using e-mail, searching the Internet, or driving a car, a person assumes the risk that the government will obtain her e-mails, Internet search terms, or the location of her car.”).

61 See Andy J. Semotiuk, Biden's First-Day 17 Executive Orders Included Major Changes To Immigration, FORBES (Jan. 22, 2021), archived at https://perma.cc/2T6T-2STQ (emphasizing the major difference between the way Donald Trump handled immigration, and the way Joe Biden is doing it). See also Michael D. Shear & Zolan Kanno-Youngs, Biden Aims to Rebuild and Expand Legal Immigration, N.Y. TIMES (Oct. 29, 2021), archived at https://perma.cc/VW7Q-7QP7 (explaining that Biden made clear during his presidential campaign that he intended to undo much of his predecessor’s immigration footprint). “[T]he Biden administration’s plans to significantly expand the legal immigration system, including methodically reversing the efforts to dismantle it by former President Donald J. Trump…” Id. But see Carrie Decell, Biden Administration Continues to Defend Social Media Registration Requirement in Court, KNIGHT FIRST AMEND. INST. COLUM. UNIV. (May 28, 2021), archived at https://perma.cc/T3N4-MLCQ (revealing that the Biden administration continued to enforce the Trump administration policy that requires millions of visa applicants each year to disclose their social media handles to the U.S. government).
screening and vetting purposes. In April 2021, the Office of Information and Regulatory Affairs ("OIRA"), the White House office that reviews federal regulations, rejected the DHS’s September 2019 proposal to collect social media identifiers on immigration forms from Visa Waiver Program applicants and applicants seeking immigration benefits.

In support of this decision, the OIRA asserted that the DHS

62 See Semotiuuk, supra note 61 (explaining that on his first day in office President Biden revoked the Muslim and African Bans previously ordered by the Trump administration); Zack Beauchamp, You're more likely to be killed by your own clothes than by an immigrant terrorist, Vox (June 26, 2017), archived at https://perma.cc/RNT5-LZHR (mentioning that Trump’s ban on travel from six Muslim majority countries was supposed to stop terrorists from getting into the U.S.). See also Proclamation No. 1014, 86 Fed. Reg. 7005, 7005 (Jan. 20, 2021) [hereinafter Presidential Proclamation] (providing President Biden’s declaration that Executive Order 13780, and Proclamations 9645, 9723, and 9983 are hereby revoked). The previous administration’s Executive Orders, which prevented individuals from Muslim and African countries from entering the U.S. are a stain on our national conscience and are inconsistent with our long history of welcoming people of all faiths and no faith at all. Id. In addition, the Secretary of State, the Secretary of Homeland Security, and the Director of National Intelligence, must provide “[a] review of the current use of social media identifiers in the screening and vetting process, including an assessment of whether this use has meaningfully improved screening and vetting, and recommendations in light of this assessment.” Id. at 7006. See also Anna Diakun, Biden Administration Signals Openness to Reconsidering Social Media Surveillance of Visa Applicants, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. (Jan. 22, 2021), archived at https://perma.cc/3KQU-2DPU (emphasizing that even as President Biden took steps to rescind a number of dangerous Trump administration policies, he also signaled how much there is left to do). “One item on the agenda: reviewing how agencies use visa applicants’ social media handles when deciding whether to allow them entry into the United States.” Id. But see Grace Dixon, Feds Say Calif. Donor Rule Can’t Prop Up Visa Policy Suit, LEXIS (Feb. 14, 2022), archived at https://perma.cc/G8P5-PG7L (noting that the report was due in May 2021, but as of February 2022 the DHS and State Department indicated that the review is still underway and they don’t expect any changes to the policy yet).

63 See Xiangnong (George) Wang, A Promising First Step Towards Curtailing Social Media Surveillance, KNIGHT FIRST AMEND. INST. COLUM. UNIV. (Apr. 27, 2021), archived at https://perma.cc/CY3U-TS9U (explaining that in an encouraging move, the OIRA denied a DHS request to collect social media information on several forms used to apply for immigration and travel benefits, which would have required an estimated 30 million applicants each year to register their social media identifiers with the DHS). See also Trent Powell, Green Card Basics: Do USCIS Officials Look at My Social Media Accounts?, TINGEN L. (Sept. 15, 2021), archived at https://perma.cc/3YCW-B96W (stating that Biden administration has rejected the DHS’s plea to continue their practice of collecting foreign national’s social media
did not adequately demonstrate the practical utility of collecting foreign national’s social media identifiers.” Although the Biden administration rejected the DHS’s collection of foreign nationals’ social media data, it has not rescinded the State Department’s corresponding collection of social media identifiers from visa applicants. Most recently, in February 2022, the Biden administration confirmed that it does not plan to make any imminent changes to the State Department’s policy. Therefore, foreign identifiers. Therefore, individuals applying for immigration benefits through DHS and USCIS are not required to submit their social media information anymore. Id. See Wang, supra note 63 (explaining that the OIRA justified the decision to reject the DHS proposal because DHS had failed to demonstrate the practical utility of collecting such information). “[I]f DHS pursues this collection in the future, it must demonstrate that the utility of registering social media information outweighs the monetary and social costs.” Id. See also Rejection of DHS Proposal, supra note 39 (indicating that the OIRA’s decision signals that there is little evidence that social media screening is an effective screening tool). See Rejection of DHS Proposal, supra note 39 (arguing that although halting the DHS collection was a big deal, it was only a first step). The Biden administration has not ended the State Department’s corresponding social media collection from about 14 million people a year who fill out visa applications. Id. “Like the DHS proposal, this State Department policy was underpinned by the Muslim ban and was justified with practically identical supporting documentation.” Id. See also Decell, supra note 61 (explaining that the Biden administration’s refusal to end the State Department’s policy is disappointing given the administration’s review of the registration requirement, as well as its recent rejection of the DHS proposal to extend the same requirement to millions more people each year). The State Department’s registration requirement is equally as unjustified as the DHS proposal, and the administration should have ended it when it had the chance. Id. See also Glenn, supra note 10 (explaining that some of the policies established in connection with the Trump administration’s Muslim ban remain in place, including the State Department requirement that visa applicants register all the social media handles that they’ve used on any of 20 specified platforms in the five years preceding their applications). This requirement is the linchpin of a surveillance system that allows the government to scrutinize visa applicants’ expressive and associational activities online even after they enter the United States.” Id. See Dixon, supra note 62 (revealing that “the Biden administration told a D.C. federal court it doesn’t expect to make ‘imminent changes’ to [the] Trump-era policy requiring visa applicants to share their social media handles.”). See also Biden Administration Tells Court It Plans to Keep Trump-Era Social Media Vetting Policy for Visa Applicants, KNIGHT FIRST AMEND. INST. COLUM. UNIV. (Feb. 11, 2022),
nationals currently applying for either immigrant and nonimmigrant visas through the State Department must still provide their social media identifiers used during the past five years on mandatory immigration and foreign traveler forms.67

B. The Current Requirements of Forms DS-160 and DS-260

When applying for a U.S. visa, foreign nationals who are not eligible for the Visa Waiver Program must submit either Form DS-160 (Online Nonimmigrant Visa Application) or Form DS-260 (Online Immigrant Visa and Alien Registration Application).68 Forms DS-160 archived at https://perma.cc/558C-46GS (noting that, despite the ongoing review of the State Department’s social media registration policy, the Biden administration advised that it did not anticipate rescinding the policy). However, just last year the Biden administration rejected the DHS’s social media collection policy, and it should do the same with the State Department’s identical policy. Id.67 See Powell, supra note 63 (indicating that individuals who apply for immigration benefits through the State Department must still submit this information on their applications forms); Chan, supra note 28 (revealing that under the State Department’s policy, nearly all U.S. visa applicants – an estimated 14.7 million people a year – will be asked to submit their social media usernames for the past five years). See also Angela Cifor, Implications of Social Media Question on DS-160 and DS-260, KOLKO & CASEY (July 15, 2019), archived at https://perma.cc/3EWQ-ZX54 (explaining that the Forms DS-160 and DS-260, the standard online application forms for applicants seeking immigrant and nonimmigrant visas to the U.S., contain a question asking for social media usernames used within the last five years for 20 popular social media websites, including Facebook, Instagram, Twitter, and YouTube). This question on Forms DS-160 and DS-260 is a good reminder that applicants seeking immigrant and nonimmigrant visas can safely assume that the State Department is carefully reviewing their social media presences. Id.67

68 See Butler, supra note 15 (explaining that generally the DS-160 form is required for applicants seeking temporary, nonimmigrant visas, including business visitors, tourists, family visitors, and temporary workers and students). On the other hand, family-based and employment-sponsored green card applicants applying from outside the United States are required to complete the DS-260 form. Id. See also DS-160: Online Nonimmigrant Visa Application, TRAVEL.STATE.GOV (Nov. 19, 2021), archived at https://perma.cc/9768-QG6W (providing that the DS-260 is for temporary travel to the U.S., and for K (fiancé(e)) visas). Form DS-160 is submitted electronically to the Department of State and is used by Consular Officers to process the visa application and, combined with a personal interview, determine an applicant’s eligibility for a nonimmigrant visa. Id. See also DS-160: Frequently Asked Questions, TRAVEL.STATE.GOV (Nov. 20, 2021), archived at https://perma.cc/N9CG-UW8A (outlining that electronically submitting your DS-160 online application is the first step in the visa application process). See also
and DS-260 (hereinafter “the Forms”) require applicants to identify and provide usernames or handles for any of approximately twenty social media accounts that they have used in the preceding five years.\(^6\) Both of the Forms contain a section titled “Social Media,” where foreign nationals are presented with a drop-down list of twenty different social media platforms and a space to input their usernames, handles, screennames, or other identifiers.\(^7\) Applicants are

Immigration Glossary, supra note 1 (defining the Visa Waiver Program as a program allowing people from 38 countries to travel to the U.S. for up to 90 days without requiring a visa).

\(^6\) See D’Arrigo & Venter, supra note 1 (noting that Forms DS-160 and DS-260 have been updated to require disclosure of social media platforms applicants used within the previous five years). Applicants must provide their usernames or handles for each platform, though passwords are not required. Id. See also 30 Day Notice of Proposed Information Collection: Supplemental Questions for Visa Applicants, 86 Fed. Reg. 8475, 8475 (Feb. 5, 2021) [hereinafter 30 Day Notice] (indicating that the State Department’s request for foreign nationals’ social media platforms and identifiers used during the last five years is now incorporated into Form DS-160). See also Social Media Case Law and the Expectation of Privacy: US v. Meregildo, BOSCO LEGAL SERV., INC. (Feb. 28, 2020), archived at https://perma.cc/LK8Q-8RP3 (revealing that from Facebook to Instagram, it is not uncommon for an individual to have a half dozen social media accounts). See also DOS Adds Social Media Questions for Visa Applicants, MYATTORNEYUSA. (Nov. 20, 2021), archived at https://perma.cc/Y82W-LHDM (noting that even applicants who do not currently use any of the listed platforms must still list their handles and identifiers if they have used any of the listed platforms within the previous five years). See also Butler, supra note 15 (explaining that the State Department’s guidance on the Forms directs visa applicants to provide information associated with all online providers/platforms and to list the usernames, handles, screennames, or other identifiers associated with their social media profiles). While foreign nationals may choose to delete social media accounts, they will still be expected to be forthcoming with required information about usernames for the last five years, and should anticipate that in some cases, a technical forensic analyst might recover deleted records. Id.

\(^7\) See D’Arrigo & Venter, supra note 1 (noting that the Forms cover “the most common U.S.-based social media platforms such as Facebook, Flickr, Google Plus, Instagram, LinkedIn, Myspace, Pinterest, Reddit, Tumblr, Twitter, Vine and YouTube; Chinese sites Douban, Qzone, Sina Weibo, Tencent Weibo and Youku; and Russian social network VKontakte.”). See also DS-260 IV Application SAMPLE, U.S. DEP’T STATE (Oct. 2019), archived at https://perma.cc/4WJY-QXAM [hereinafter DS-260 Sample] (illustrating the social media questions included in the Form, which request that applicants select from the drop-down list
subsequently asked if they wish to provide information about their presence on any other websites or social media platforms, which were not included in the drop-down list, but that they have used within the last five years to create or share content.\textsuperscript{71}

While applicants have the option to select “none,” indicating that they do not have a social media presence on any of the listed social media platforms, foreign nationals who choose this option will undoubtedly be further scrutinized.\textsuperscript{72} In addition, applicants who falsely select “none” or who do not provide their social media information fully and truthfully, may receive a denial of their application or potentially become subject to an accusation of fraud or willful misrepresentation.\textsuperscript{73} When an applicant signs the end of their each social media platform they have used within the last five years). Applicants are provided with the ability to click “add another” to add up to as many social media platforms as they need. \textit{Id. See also Online Nonimmigrant Visa Application DS-160 EXEMPLAR, U.S. DEPT' STAE (Nov. 19, 2021), archived at https://perma.cc/SMR8-5D7W [hereinafter DS-160 Sample] (clarifying that applicants must list the username, handle, screenname, or other identifiers associated with their social media profiles, but do not need to list accounts designated for use by multiple users within a business or other organization). Applicants have the option to select “NONE” if they do not have a social media presence. \textit{Id.}

\textsuperscript{71} See DS-160 Sample, supra note 70 (showing that applicants can respond either “yes” or “no” to the question regarding their presence on any other websites or applications used to create or share content such as photos, video, status updates, etc.). If applicants respond yes, they are asked to provide the name of the platform and their username or handle, but need not include private messaging or person-to-person messaging services such as WhatsApp. \textit{Id. See also DS-260 Sample, supra note 70 (showing the same question regarding an applicant’s presence on any other websites or applications used to create or share content posed to applicants).}

\textsuperscript{72} See Butler, supra note 15 (highlighting that if the question is left unanswered, the system does not permit the applicant to proceed on the form). While there is an option of answering “none,” “an applicant who answers ‘none’ undoubtedly will be scrutinized at the visa interview, and the consular officer very likely will have independently searched for an online presence of the applicant and may challenge whether the answer was accurate.” \textit{Id. See also DS-160: Frequently Asked Questions, supra note 68 (noting that all mandatory questions must be answered and the system will not allow an applicant to submit an application with any mandatory questions left unanswered); Dobrina Ustun, What you need to know about Social Media Information requirements while filing DS-160, or DS-260 forms?, USTUN L. GROUP (Sept. 18, 2019), archived at https://perma.cc/6QD6-Z3A7 (emphasizing that providing social media information is mandatory for all nonimmigrant visas).}

\textsuperscript{73} See DOS Adds Social Media Questions for Visa Applicants, supra note 69 (revealing that “[f]ailure to provide accurate and truthful responses on a visa application or during a visa interview may result in denial of the visa by a consular
DS-160 or DS-260 Form, they certify that they understand that any willfully false or misleading statement or willful concealment of a material fact may result in refusal of their visa, permanent exclusion from the U.S., or criminal prosecution and/or deportation. In addition, under the Immigration and Nationality Act, 212(a)(6)(C)(i), “[a]ny Alien who, by fraud or willfully misrepresenting a material fact, seeks to procure (or has sought to procure or has procured) a visa, other documentation, or admission into the United States or other benefit provided under this Act is inadmissible.” While applicants must

If the applicant chooses the option ‘none’ as his or her reply when it is not a truthful answer, the response could expose in certain circumstances the applicant to denial of the application and, worse, potentially to an accusation of fraud or willful misrepresentation if the failure to disclose the information ‘tends to shut off a line of inquiry which is relevant to … eligibility and which might well have resulted in a proper determination that he or she be inadmissible.’

See DS-160 Sample, supra note 70 (stating that “[t]he submission of an application containing any false or misleading statements may result in the permanent refusal of a visa or the denial of entry to the United States.”). “All declarations made in the application are unsworn declarations made under penalty of perjury.” Id. See also DS-260 Sample, supra note 70 (showing that applicants must sign to certify that they understand that any willfully false or misleading statement or concealment of a material fact may result in refusal of visa, denial of admission to the U.S., or subject them to criminal prosecution and/or removal from the U.S.).

75 See Waivers for Fraud or Willful Misrepresentation of a Material Fact to Obtain an Immigration Benefit, MYATTORNEYUSA (Nov. 20, 2021), archived at https://perma.cc/8B56-CJ3E (stressing that if a foreign national is caught using fraud or willful misrepresentation of a material fact to procure an immigration benefit, he or she will be deemed inadmissible to the U.S. for life). See also 212(a)(6)(C)(i) Material Misrepresentation / Fraud, WHITE & ASSOCIATES (Nov. 20, 2021), archived at https://perma.cc/PZ22-4E9D [hereinafter Material Misrepresentation / Fraud] (revealing that material, willful misrepresentation or fraud is the second most popular grounds for inadmissibility among consular officers). In the visa context, section 212(a)(6)(C)(i) requires three elements: (1) the visa applicant made a misrepresentation; (2) the visa applicant made this misrepresentation willfully; and (3) the visa applicant’s misrepresentation was material. Id. Even if an applicant does
therefore take care to accurately and thoroughly detail all social media identifiers they have used within the past five years, many foreign nationals have expressed concern and confusion while completing the Forms.\footnote{76}{See Material Misrepresentation / Fraud, supra note 75 (emphasizing that the consequences for making a misrepresentation are draconian: a lifetime bar from the U.S.); Cifor, supra note 67 (revealing that any misrepresentation or material omission is considered fraud, and thus applicants must truthfully disclose information related to their social media presence in the past five years). But see @mljedi, REDDIT (Feb. 22, 2020), archived at https://perma.cc/96DY-PW4Y (revealing confusion as to whether it is only necessary to provide main social media platforms and identifiers on Form DS-160, or if one must also include fake Instagram accounts, Reddit throwaways, empty Facebook accounts, business accounts, deactivated Twitters, or forms of online presence that use one’s nicknames). It is unreasonable to have to list absolutely everything. Id. See also @Bach_Hy_2001, REDDIT (Mar. 18, 2020), archived at https://perma.cc/M4LM-4RCK (emphasizing that he/she has been worrying about how to properly complete the social media section of Form DS-160 for quite some time since beginning to fill it out). See also @S11pstre4m, REDDIT (Oct. 24, 2021), archived at https://perma.cc/C5JE-7WCE (addressing concerns that the requirement to provide social media information on Form DS-160 is way too invasive). See also Supporting Statement, supra note 7, at 15 (highlighting that even sophisticated social media users do not always remember all their social media identifiers and can easily forget that they own certain accounts).}

C. Recent Freedom of Information Act Requests and Lawsuits Against The Government

While the information that foreign nationals must provide is clearly laid out in Forms DS-160 and DS-260, it is less clear how the government scrutinizes social media data when determining who can enter or stay in the country.\footnote{77}{See Complaint at 2, Ctr. for Democracy & Tech. v. U.S. Dep’t Homeland Sec., No. 1:21-cv-00134 (D.C. Jan. 15, 2021) [hereinafter CDT Complaint] (noting the limited information about the DHS’s social media monitoring that is publicly available). The lack of such publicly available information causes concern that the social media monitoring policies are of dubious constitutionality, and may have the effect of chilling of Americans’ speech on social media platforms. Id.} In recent years, a number of organizations have submitted Freedom of Information Act (“FOIA”) requests to compel the government to turn over documents detailing not know English and misunderstands a question, the inaccurate information is still considered a misrepresentation. \textit{Id.} “[T]he term ‘material’ means a misrepresentation which might have led a consular officer to find a person ineligible for a visa.” \textit{Id.}
how they use foreign national’s social media data.\textsuperscript{78} A FOIA request is a request submitted to a federal agency asking for records on a specific topic, which compels that agency to produce requested records unless they fall within one of nine narrow exemptions.\textsuperscript{79} In justifying the grounds for their FOIA requests against the DHS and State Department, organizations have argued that “[t]he public deserves to know how the government scrutinizes social media data when deciding who can enter or stay in the country,” and that there is “an urgent need

\textsuperscript{78} See id. (explaining that FOIA requests were made to investigate and better understand the DHS’s social media monitoring programs and practices). See also ACLU Found. v. United States DOJ, No. 19-cv-00290-EMC, 2021 U.S. Dist. LEXIS 181279, at *3 (N.D. Cal. Sep. 22, 2021) (explaining that on May 24, 2018, Plaintiffs submitted FOIA requests to Defendants to obtain records pertaining to their social media surveillance programs, including the monitoring and retention of immigrants' social media information for the purpose of conducting ‘extreme vetting.’); ACLU V. DOJ: FOIA LAWSUIT SEEKING INFORMATION ON FEDERAL AGENCIES’ SURVEILLANCE OF SOCIAL MEDIA, ACLU (Mar. 26, 2019), archived at https://perma.cc/AGH2-RVCW (arguing that the public deserves to know how government agencies are surveilling online speech, what policies apply to such surveillance, and how such policies impact individuals’ rights).

\textsuperscript{79} See Theodore Z. Wyman, Disclosure of Surveillance Records Under Freedom of Information Act, 5 U.S.C.A. § 552(b)(7)(E), 64 A.L.R. Fed. 3d 8 (Nov. 20, 2021) (noting that FOIA requires an agency, within 20 days of receiving a request for records, to determine whether to produce responsive records and to immediately notify the requester of the agency’s determination). The basic purpose of the FOIA is “to ensure an informed citizenry that is vital to the functioning of a democratic society and that is needed to check against corruption and to hold the governors accountable to the governed.” Id. Agencies must produce requested records unless they fall within one of the narrow exemptions set forth in the statute. Id. See also Freedom of Information Act (FOIA) Reference Guide (2018), NAT’L ARCHIVES (Nov. 20, 2021), archived at https://perma.cc/8UXK-WG82 (describing that the Freedom of Information Act, or FOIA generally provides any person with the statutory right, enforceable in court, to obtain access to government information in executive branch agency records). There are the nine FOIA exemptions and a FOIA request will be denied in whole or in part only when it is determined that disclosure of information would harm an interest protected under one or more of the nine FOIA exemptions. Id. However, FOIA requesters may appeal any such withholding, or other adverse decision, back to the agency, and may also file a lawsuit to seek redress in federal court. Id.
to understand the nature, extent, and consequences of that surveillance.\textsuperscript{80} However, the DHS and State Department have been reluctant to respond to FOIA requests and produce documents to the public, resulting in multiple lawsuits filed by various organizations against the agencies.\textsuperscript{81} In the most recently decided lawsuit filed by the American Civil Liberties Union Foundation (“ACLU”), the U.S. District Court for the Northern District of California ordered seven federal agencies – including the DHS and the State Department – to produce unredacted versions of certain documents that did not meet any of the agencies’ needs.

\textsuperscript{80} See CDT Files Lawsuit Against DHS for Information on Social Media Monitoring at the Border, CTR. DEMOCRACY \& TECH. (Jan. 19, 2021), archived at https://perma.cc/5QX9-NTF2 (quoting CDT General Counsel Avery Gardiner). See also Mana Azarmi \& Avery Gardiner, CDT Files FOIA Lawsuit Demanding Information on How DHS Looks at Social Media for Immigration and Naturalization, CTR. DEMOCRACY \& TECH. (Jan. 19, 2021), archived at https://perma.cc/YK73-6TQ5 (explaining that the Center for Democracy \& Technology (“CDT”) made the FOIA requests to investigate and better understand the DHS’s social media monitoring practices). CDT is a 25-year-old nonpartisan nonprofit organization working to promote democratic values by shaping technology policy and architecture. Id. See also CDT Complaint, supra note 77, at 2 (highlighting that CDT brings this action to enforce its rights and the public’s right to receive information about the DHS’s social media monitoring practices). See also Complaint at 2, ACLU Found. v. United States DOJ, No. 3:19-cv-00290 (N.D. Cal. Jan. 17, 2019) [hereinafter ACLU Complaint] (asserting that the public interest in the release of records regarding the government’s social media monitoring practices is clear). “Because the government’s growing use of social media surveillance implicates the online speech of millions of social media users, U.S. citizens and residents of all backgrounds have an urgent need to understand the nature, extent, and consequences of that surveillance.” Id. at 2–3.

\textsuperscript{81} See CDT Files Lawsuit Against DHS for Information on Social Media Monitoring at the Border, supra note 80 (indicating that CDT filed the lawsuit in a Washington, D.C. federal court after DHS failed to respond to CDT’s FOIA requests for more than a year). “We are holding the government to its FOIA obligations in order to better understand these constitutionally dubious practices.” Id. See also Nyczepir, supra note 9 (noting that despite the transition to the Biden administration, the CDT intends to continue to pursue its case against the Trump administration). See also Nicholas Iovino, Judge questions withheld records on US social media surveillance programs, COURTHOUSE NEWS SERV. (July 2, 2021), archived at https://perma.cc/8K8D-HCSJ (explaining that in January 2019, the ACLU sued seven federal agencies for refusing to release records on their use of social media monitoring tools). See also ACLU Found., 2021 U.S. Dist. LEXIS 181279, at *2–3 (providing the factual background behind the lawsuit and ACLU’s arguments against Defendants).
alleged FOIA exemptions. Some additional documents and information will therefore become publicly available, but the lack of complete transparency prevents the public from fully understanding how their online speech, associations, and activities were, and continue to be, monitored.

IV. Analysis

The number of FOIA requests and lawsuits filed against the DHS and State Department is indicative of the urgent need for more information on the social media monitoring policies of these agencies. In our current digital age, simply requiring that individuals

---

82 See ACLU Found., supra note 81, at *9 (explaining that the Court reviewed the documents at issue for each agency *in camera* and determined whether the exemptions applied or not). Following the *in camera* review, the Court ordered the defendants to produce unredacted versions of certain documents within fourteen days of their order. *Id.* at 24. See also *In Camera Law and Legal Definition*, US LEGAL (Dec. 30, 2021), archived at https://perma.cc/N5D8-RA8K (explaining that *in camera* is a Latin term meaning “in chambers” and refers to a hearing or discussions with the judge in the privacy of his chambers or when spectators and jurors have been excluded from the courtroom). During an *in camera* examination, the judge will review the confidential or sensitive information and determine whether to introduce it to the jury and make it part of public record. *Id.*

83 See Scott, supra note 10, at 157 (emphasizing that the government is secretive about the methods used for social media monitoring, the vastness of the data collection, and the algorithms used to analyze the data). “Such secrecy prevents the public from understanding the extent of the monitoring of social media, whether the algorithms produce bias results, or even if the social media monitoring is effective by any measure.” *Id.* See also *Social Media Monitoring*, supra note 7 (arguing that the documents disclosed by the government are often jargon-filled and do not provide sufficient details or context to confirm the effectiveness or risks of such programs).

84 See ACLU Complaint, supra note 80, at 2 (asserting that the public interest in the release of records regarding the government’s social media monitoring practices is clear). “Because the government’s growing use of social media surveillance implicates the online speech of millions of social media users, U.S. citizens and residents of all backgrounds have an urgent need to understand the nature, extent, and consequences of that surveillance.” *Id.* at 2–3. See also *CDT Files Lawsuit Against DHS for Information on Social Media Monitoring at the Border*, supra note 80 (arguing that “[t]he public deserves to know how the government scrutinizes
disclose their social media identifiers to the government threatens to infringe on their Constitutional right to privacy and chill their free speech and association. On top of that, however, the lack of information about how the State Department scrutinizes and retains foreign nationals’ social media data further exacerbates these Constitutional concerns and allows for discriminatory pretextual denials of immigration petitions.

social media data when deciding who can enter or stay in the country.

“Government surveillance has necessary limits, particularly constitutional ones.” Id. See also Social Media Monitoring, supra note 7 (emphasizing that it is critical for the public to understand the ways in which the government exploits social media).

See Social Media Monitoring, supra note 7 (noting that the deleterious effect of surveillance on free speech has been well documented in empirical research). In a survey of a representative sample of U.S. internet users, 62 percent reported that they would be much less or somewhat less likely to touch on certain topics if the government was watching, and 78 percent of respondents stated that they would be more cautious about what they said online. Id. at n.14. In addition, studies found that users from countries outside the U.S. were less likely to search using terms that they believed might get them in trouble with the U.S. government. Id. See also Rejection of DHS Proposal, supra note 39 (arguing that there is evidence that social media surveillance discourages people from freely speaking and associating online).

See also Handeyside, supra note 35 (revealing that the chilling effect of social media monitoring is not just speculation, and that research proves “that people self-censor and avoid controversy when they know the government is watching.”). See also @Slipstream, supra note 76 (explaining that although their social media profiles are mostly set to private, they are still watching what they post).

See Blue, supra note 5 (noting that the social media monitoring policy avoids detailing the method of collection or security of storage of foreign nationals’ data). See also CDT Complaint, supra note 77 (arguing that the limited information about the governments’ practices that are publicly available has the effect of chilling Americans’ speech on social media platforms). In addition, social media monitoring opens the door to discriminatory pretextual denials of benefits, which the government has even acknowledged. Id. See also Social Media Monitoring, supra note 7 (noting that there is limited information on what the State Department’s review of applicants’ social media activity will entail). Much of the information on social media monitoring and the ways in which the data collected is used is buried in jargon-filled notices about changes to document storage systems that impart only the vaguest outlines of the underlying activities. See also Miller, supra note 2, at 405–06 (arguing that the government’s use of social media surveillance can lead to racial targeting and greater scrutiny of individuals based on a single post).
A. The Lack of Information on Social Media Monitoring Policies Infringes on Foreign Nationals’ and U.S. Citizens’ Constitutional Rights and Harms Public Discourse

1. First Amendment: The Chilling Effect on Free Speech and Association

Although the State Department’s current social media collection and monitoring policy does not directly forbid certain types of speech or associations, it undoubtedly has a chilling effect on both foreign nationals’ and U.S. citizens’ online activity.\(^\text{87}\) Knowing that they must provide their social media identifiers in order to apply for a visa, foreign nationals will feel dramatically deterred from speaking freely and engaging with others online for fear that their activity will be misinterpreted and negatively impact their application.\(^\text{88}\) In

\(^{87}\) See Glenn, supra note 10 (referring to the social media data collection policy as a dragnet that has a dramatic chilling effect on the speech and associations of millions of people around the world). See also Miller, supra note 2, at 417–18 (explaining that the collection of social media handles creates a chilling effect on a foreign national’s speech and ability to associate with organizations and other affiliations). Ultimately, the policy denies foreign national’s the freedom to freely associate and speak without the fear of repercussions. Id. See also Doc Society v. Blinken, supra note 36 (asserting that the State Department’s registration requirement and related retention and dissemination policies violate the First Amendment because they deprive visa applicants of the rights to anonymous speech and private association, and because they chill constitutionally protected speech and association).

\(^{88}\) See Glenn, supra note 10 (stressing that the registration requirement deters people who decide to apply for U.S. visas from freely sharing their views and engaging with others on social media, for fear that their speech will be misinterpreted or used against them). “At the same time, it also deters other people from even applying for a U.S. visa to come to the United States in the first place, because they don’t want to have to subject their online speech to this U.S. government surveillance.” Id. See also Rejection of DHS Proposal, supra note 39 (explaining that people will self-censor when they reasonably fear that their speech will be misinterpreted). See also Social Media Monitoring, supra note 7 (arguing that social media monitoring will impact what people say online, leading to self-censorship of people applying for visas as well as their family members and friends). See also Decell & Panduranga, supra note 35 (noting that foreign nationals must now consider whether certain speech will lead U.S. officials to subject their visa applications to additional scrutiny, delay the processing of those applications, or deny the applications altogether).
addition, the State Department’s failure to disclose what constitutes a national security concern or is considered grounds for denying a foreign national’s visa petition, causes foreign nationals to self-censor to an even greater extent. Foreign nationals, unaware of what types of speech could be flagged by the government, will feel it necessary to restrict speech on many different topics, including political and religious beliefs, opinions on the U.S. administration, and general social commentary.

While individuals may take steps such as utilizing a social media platform’s privacy settings and limiting access to their social media information, it is commonly known that nothing a person posts online is ever guaranteed to remain confidential. In addition, foreign

89 See Waheed, supra note 8 (explaining that “a program ostensibly designed to identify ‘national security concerns’ has been underway, apparently without basic standards or guidance as to what constitutes such a ‘concern.’”). See also Handeyside, supra note 35 (mentioning the lack of published standards on how the government reviews and uses a foreign national’s social media data). See also Scott, supra note 10, at 157 (highlighting that the chilling effect on foreign nationals’ First Amendment rights is exacerbated by the secrecy behind the methods the government uses for social media monitoring). Such secrecy prevents the public from understanding the extent of the monitoring of social media. Id.

90 See Handeyside, supra note 35 (highlighting that when people don’t know what kind of speech will get them into trouble, they self-censor to an even greater extent). See also Rejection of DHS Proposal, supra note 39 (presenting an example of a foreign national who felt compelled to delete posts criticizing the current U.S. administration out of fear that the posts would delay approval of their visa application). People may refrain from being critical of the government online when they are subject to surveillance, since they have legitimate reason to fear being penalized for their speech. Id. See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (presenting an example of an individual who was detained and interrogated about his online presence and involvement with Black Lives Matter). This case reveals that government authorities are attentive to the political views of those seeking entry to the U.S. Id.

91 See Everything You Need to Know About the New DHS Social Media Policy, supra note 1 (explaining that DHS claims it only looks at publicly available information and is not able to access social media accounts set to private). However, a person’s social media activity may not be as private as he/she thinks. Id. On Facebook, for instance, tagging a friend in posts and photos means all of their friends can see it too. Id. See also Social Media Case Law and the Expectation of Privacy: US v. Meregildo, supra note 69 (noting that even if a social media user does have strict privacy settings that allow only “friends” to view posts, they cannot guarantee that this information remains private, as their “friends” can share the content they have access to with whoever they want). See also @Sl1pstre4m, supra note 76 (explaining that although their social media profiles are mostly set to private, they are still watching what they post).
nationals who choose to change their social media names or use a pseudonym in hopes of evading government surveillance must now surrender their anonymity under the State Department’s social media identifier registration requirement.92 The inability to hide their social media content or evade government surveillance leaves foreign nationals with no option but to self-censor or limit their social media activity altogether.93 Even foreign nationals who know that they have

92 See Decell & Panduranga, supra note 35 (stating that the chilling effects of the registration requirement are particularly pronounced for individuals who use pseudonymous social media handles).

Some [people] use pseudonymous social media handles to conduct research in sensitive online communities, to avoid stalkers and trolls in public forums, to promote or participate in political demonstrations, or to speak out against their own governments. The registration requirement forces these individuals to surrender their anonymity and accept the risk that their handles will end up in the hands of rights-abusing governments, hackers, and others. *Id.*

93 See Scott, supra note 10, at 155–56 (explaining that many individuals who have become aware of government surveillance programs have taken steps to shield their information from the government, including self-censoring, changing social media privacy settings, using social media less, and avoiding certain terms in online communications). *See also Social Media Surveillance, supra note 27 (arguing that awareness or fear of government surveillance of the internet can have a substantial chilling effect on internet users).* “Thus, as individuals wishing to visit or immigrate to the United States realize that they will need to disclose their social media handles, they may censor themselves in order to improve their chances of obtaining visas.” *Id.*

*See also Glenn, supra note 10 (presenting the argument that if people are forced to disclose their pseudonymous social media handles and give up their right to online*
nothing to hide are still likely to self-censor their online speech and activity when they know that the government will collect and monitor their social media data.94

The State Department’s social media monitoring policy also has a chilling effect on foreign nationals’ and U.S. citizens’ right to free association.95 An individual’s connections on social media – including their followers or friends and their engagement with political or ideological groups – are intimate and expressive associations that warrant protection under the First Amendment.96 However, the lack

anonymity, they may simply decide not to come to the U.S. for fear about this information ending up in the wrong hands). “Alternatively, they may still need to come to the United States and, as a result, will just stop using social media in order to protect themselves from whatever reprisals they might otherwise suffer.” Id. See also Rejection of DHS Proposal, supra note 39 (presenting an example of one member of a documentary filmmaker organization who reviewed three years of social media activity and deleted posts criticizing the current U.S. administration out of fear that the posts would delay approval of their visa application). Another member of the same documentary filmmaker organization chose to completely stop expressing his opinions and views and interacting with others on social media. Id. 94 See Rejection of DHS Proposal, supra note 39 (highlighting that when people are aware that the government is watching, they are likely to self-censor regardless of whether they actually have anything to hide). See also Doc Society v. Blinken, supra note 36 (explaining that even people who do not choose to use pseudonymous handles to speak online about sensitive or important topics may “reasonably fear that government officials will misinterpret or misattribute posts made in online environments where people interact differently than they do in real life.”).

95 See Glenn, supra note 10 (calling the State Department’s social media registration policy the linchpin of a surveillance system that allows the government to scrutinize visa applicants’ expressive and associational activities online). The policy creates what is, in effect, a social media dragnet that chills the association of millions of people around the world. Id.

96 See WHAT'S YOUR SOCIAL MEDIA FOOTPRINT AND WHY DOES IT MATTER?, supra note 5 (noting that a social media footprint also contains a person’s network of associations to different people, groups, and ideas that they have created for themselves); Stop Collecting Immigrants’ Social Media Data, supra note 5 (indicating that a foreign national’s social media activity reveals that person’s network of friends, relatives and co-workers, some close and some distant). See also Boy Scouts of Am. v. Dale, 530 U.S. 640, 648 (2000) (emphasizing that the First Amendment's protection of expressive association is not reserved only for advocacy groups, but for any group that engages in some form of expression, whether it be public or private). See also Sabin, supra note 46, at 724 (revealing that social media platforms such as Facebook are expressive associations). “Facebook literally organizes groups of individuals according to educational, geographic, political, and religious categories. In this sense, Facebook is the digital analog to traditional
of public information and broad scope of the State Department’s social media monitoring policy allows the government to sweep up and review social media data of those connected with a foreign national, including U.S. citizens who did not provide the government their social media identifiers.\textsuperscript{97} In turn, a foreign national’s application could be negatively impacted by their interactions with various associations or the online activity of their followers.\textsuperscript{98} This reality is particularly concerning given the fact that social media users do not have control over the posts or activity of their followers, and may be organizations such as the NAACP and Boy Scouts.” \textit{Id.} In addition, highly personal Facebook connections might qualify as intimate associations. \textit{Id.} at 725 n. 176. \textsuperscript{97} See Social Media Monitoring, supra note 7 (explaining that a social media check can also extend to associates who posted on or interacted with an applicant on their social media profile, which could include Americans and other contacts living in the U.S.). Although the social media monitoring policy targets foreign nationals, it also sweeps up information about American friends, family members, and business associates, either deliberately or as a consequence of its broad scope. \textit{Id.} See also Social Media Surveillance, supra note 27 (revealing that individuals who already live in the U.S. under visas could have their social media content, as well as their online communications with U.S. citizens, subjected to scrutiny). See also Blue, supra note 5 (emphasizing that the social media monitoring policy will affect all of us, including U.S. citizens). It is very likely that you have friend, family member, or colleague who was not born in the U.S. \textit{Id.} “And even if you don't personally know someone… you'll most certainly show up in those millions of files somewhere as a ‘like’ or other piece of tangential social metadata.” \textit{Id.} See also Rodil, supra note 4, at 270 (noting privacy advocates concern that the social media monitoring could pull information about American citizens who communicate and interact with immigrants over social media). See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (arguing that although the government claims it has directed “[c]onsular staff…to take particular care to avoid collection of third-party information,” such collection and analysis will be inevitable.”). \textsuperscript{98} See Supporting Statement, supra note 7, at 10 (citing concern on the impact that a foreign nationals’ associations, friendships, or likes on social media can have on a visa application). For example, a Pulitzer Prize-nominated journalist who reports on extremist groups may connect with sources through social media platforms. \textit{Id.} However, an immigration agent looking at her social media presence out of context might misunderstand the nature of such online relationships. \textit{Id.} See also D’Arrigo & Venter, supra note 1 (explaining that the application of the State Department’s social media monitoring policy is “so broad that in some cases, even posts or comments made by other ‘connections’ or ‘friends’ on the applicant’s social media platforms can affect the ability to obtain an immigration benefit or gain admission into the U.S.”).
connected to individuals they do not actually know and whose opinions they do not actually agree with. As a result, foreign nationals – unaware of what online associations could negatively impact their application – may choose to stop interacting with certain friends, leave certain groups, or delete their social media accounts altogether.

Government surveillance that chills the free speech and association of individuals on social media threatens to harm public discourse in one of the most important spaces for exchange of views. Social media platforms offer an important forum for foreign nationals

---

99 See D’Arrigo & Venter, supra note 1 (providing an example that in 2019, an incoming Harvard University student from Lebanon was “refused entry at the border, not because of posts he had authored himself, but rather because individuals on his list of ‘friends’ had posted political points of view on social media that were deemed to be opposed to the U.S.”). The student did not even “like,” comment on, or share the posts. Id. See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (noting that some people may follow or interact with individuals with provocative or even reprehensible views for purposes of research and public education). For instance, a foreign journalist who interacts with a provocative tweet from an ISIS follower in order to find it again more easily for a piece of writing may be flagged as a supporter of the poster’s positions. Id. See also Rejection of DHS Proposal, supra note 39 (revealing that there is evidence that social media surveillance discourages people from freely speaking and associating online). See also Decell & Panduranga, supra note 35 (emphasizing that because of the registration requirement, some individuals have left online groups, stopped interacting with certain friends online, or deleted their social media posts or accounts completely). See also D’Arrigo & Venter, supra note 1 (noting that visa applicants should be mindful of who they with associate on social media, especially individuals who are vocal about controversial political issues, or those demonstrating anti-U.S. government views).

100 See Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017) (holding that it is clear that cyberspace, and in particular social media, is the most important place for the exchange of views). See also Decell & Panduranga, supra note 35 (holding that social media is interconnected and international in ways that profoundly benefit American cultural life). Therefore, subjecting individuals’ social media profiles to mass surveillance threatens the creative freedom and potentially even the lives of artists and activists around the world. Id. See also Campbell, supra note 29, at 517 (explaining that essentially all of our communication takes place via the internet, and as a result, social media has become the bedrock of American culture). See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (emphasizing that many people around the world use social media to support democratic movements and to campaign for political reform). “Mandating the disclosures proposed will concretely damage movements for self-governance and American cultural and economic dynamism, particularly if other countries follow U.S. precedent and impose similar requirements.” Id.
and U.S. citizens to engage in a wide variety of protected First Amendment activity, such as promoting or participating in political discourse, voicing their opinions, or speaking out against their own governments. Not only does the State Department’s social media monitoring policy therefore prevent individuals from feeling safe to express their personal opinions or connect with diverse people or groups, it is also detrimental in that it deprives audiences, including U.S. citizens, of opportunities to hear from and interact with other individuals.

102 See Decell & Panduranga, supra note 35 (noting that the Supreme Court has recognized that “social media platforms offer the most important spaces for people to participate in the ‘modern public square’ or otherwise explore ‘the vast realms of human thought and knowledge.’”). People use social media to discuss an array of social and political issues, including corruption, human rights atrocities, women’s rights, climate change, racial injustice, and the global impact of U.S. policy. Id. See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (emphasizing that “social media facilitates the free exchange of ideas that is a hallmark of an open democratic society.”). For many, social media is “the principal source for knowing current events, … speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge.” Id. See also Reno v. Am. C.L. Union, 521 U.S. 844, 870 (1997) (explaining that the internet provides relatively unlimited, low-cost capacity for communication of all kinds). “Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.” Id. See also Packingham, 137 S. Ct. at 1732 (commenting on how social media users are able to engage in a wide array of protected First Amendment activity). Social media allows users to engage on any number of diverse topics and communicate with one another on any subject that might come to mind. Id. “On Facebook, for example, users can debate religion and politics with their friends and neighbors or share vacation photos. On LinkedIn, users can look for work, advertise for employees, or review tips on entrepreneurship. And on Twitter, users can petition their elected representatives and otherwise engage with them in a direct manner.” Id. at 1735.

103 See Glenn, supra note 10 (revealing that the Supreme Court has held that people in the U.S. have a right to hear from people from outside the U.S.). Ultimately, the chilling effect of the registration requirement impacts not only those speaking, but also those listening to others. Id. For example, Doc Society and the International Documentary Association are leading U.S.-based documentary film organizations that routinely invite filmmakers from around the world to come speak to U.S.
2. Threats to Foreign Nationals’ and U.S. Citizens’ Fourth Amendment Right to Privacy

The State Department’s social media collection and monitoring policy also threatens foreign nationals’ and U.S. citizens’ right to privacy under the Fourth Amendment. An individual’s social media profile can reveal deeply personal data and information on almost every aspect of their life, such as their hobbies, relationship status, sexual orientation, and political and religious beliefs. Forms DS-...
160 and DS-260 currently require applicants to provide handles for approximately twenty common social media accounts such as Facebook, Instagram, and Twitter; however, the State Department has the ability to add additional platforms to the list. Therefore, the State Department could update the Forms and theoretically go so far as to request social media identifiers from platforms that reveal even more intimate and personal details, such as Tinder or OkCupid.

Under the State Department’s social media collection policy, the agency can also retain foreign nationals’ social media information indefinitely, share it broadly among federal agencies, and, in some circumstances, disclose it to foreign governments. Technically, under current Fourth Amendment analysis, the third-party doctrine could have search histories, Twitter rants, YouTube binges, and Facebook profile information” collected).

See D’Arrigo & Venter, supra note 1 (noting that the Forms cover “the most common U.S.-based social media platforms such as Facebook, Flickr, Google Plus, Instagram, LinkedIn, Myspace, Pinterest, Reddit, Tumblr, Twitter, Vine and YouTube; Chinese sites Douban, Qzone, Sina Weibo, Tencent Weibo and Youku; and Russian social network VKontakte.”). But see Supporting Statement, supra note 7, at 5 (revealing that if approved by the OMB, the State Department may update the list of platforms).

See Supporting Statement, supra note 7, at 22 (highlighting that the platforms listed on the State Department’s Forms may be updated by the Department by adding or removing platforms). See also Blue, supra note 5 (revealing that the large amount of intimate and personal information available on platforms such as Tinder is shocking).

See Decell & Panduranga, supra note 35 (explaining that after being collected, foreign nationals’ social media data is then “retained indefinitely, shared widely within the federal bureaucracy as well as with state and local governments, and, in some contexts, even disseminated to foreign governments.”). See also Social Media Monitoring, supra note 7 (revealing that USCIS’s A-files, which can include social media information, are stored for 100 years after the individual’s date of birth); Social Media Surveillance, supra note 27 (noting that the DHS and State Department can share social media information with other law enforcement and security agencies without limits on re-dissemination). See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (mentioning that the State Department has explained the “information obtained from applicants…is considered confidential and is to be used only [purposes related to] the immigration, nationality, and other laws of the United States…”). However, the State Department has not provided enough information on how it will use, store, or share the data it obtains, or for what other purposes outside of immigration the data could be used. Id.
allows the government to collect and store social media information without violating an individual’s right to privacy as there is no reasonable expectation of privacy in information disclosed on social media platforms.\textsuperscript{109} Although the Supreme Court has yet to decide how the third-party doctrine will impact social media data, it is well-argued that the third-party doctrine is outdated and unsuitable in our digital age.\textsuperscript{110}

The introduction of social media has caused individuals to share far more information with third parties than they were even remotely capable of in 1979, when the third-party doctrine was introduced.\textsuperscript{111} In addition, individuals are now able to limit the

\textsuperscript{109} See Campbell, supra note 29, at 530 (stating that the third-party doctrine essentially allows the government to collect a person’s social media information without a warrant and without any Fourth Amendment considerations). See also Bedi, supra note 57 at 2–3 (explaining that almost all communications over the Internet and on social media are stored for some period of time on third party servers or Internet service providers known as ISPs, and therefore, users basically lose any Fourth Amendment protection in these online communications). Under a strict application of the third-party doctrine, a social media user would lose Fourth Amendment protection for any information transmitted through the social media platform because the user has knowingly disclosed it to a third party’s storage system). Id. at 15–16.

\textsuperscript{110} See Bedi, supra note 57, at 17–18 (indicating that the Supreme Court has not yet ruled on how the third-party doctrine will impact communications transmitted through social networking sites.). But see Gee, supra note 59, at 287 (noting that since being established, “the third-party doctrine ‘may be the most critiqued aspect of Fourth Amendment jurisprudence.’”). See also Campbell, supra note 29, at 530 (describing the third-party doctrine as a “controversial and antiquated” policy that has received modern pushback). Many scholars acknowledge the inherent problems resulting from the third-party doctrine. Id. at 531. For example, Professor Stephen E. Henderson argues that the third-party doctrine is controversial and “fundamentally misguided.” Id.

\textsuperscript{111} See Miller, supra note 2, at 414 (emphasizing that as a result of social media, individuals share far more with third parties than they did in 1979). Unlike in 1979, individuals now share GPS location data, acquaintance information, various thoughts in the form of status updates, personal photos, and political opinions. Id. As a result, the traditional assumption of risk assumed in third-party doctrine cases is no longer realistic when applied to many new technologies. Id. at 415. See also United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (explaining that in the digital age, people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks). See also Gee, supra note 59, at 289 (noting that Chief Justice Roberts questioned the viability of the third-party doctrine \textit{in dicta} by pointing out the clear difference between the limited types of personal information found in 1970s era bank records and landline phone records,
invasion of privacy of their personal information on social media, by taking steps such as restricting their privacy settings or using a pseudonym when creating their social media account. These steps not only increase an individuals’ subjective expectation of privacy on social media, but should also increase society’s willingness to view this expectation of privacy as reasonable and therefore protected under the Fourth Amendment. Ultimately, although the third-party doctrine currently allows the government to review and monitor foreign nationals’ social media accounts, the doctrine as a whole is 

and the exhaustive chronicle of communicative content casually collected by wireless carriers today).

112 See Scott, supra note 10, at 155–56 (highlighting that individuals will take steps to shield their information from the government). For instance, social media users can change their privacy settings in order to restrict access to their information. Id. See also Jackson, supra note 57 (noting how individuals can utilize the available privacy settings on Facebook and other social media platforms to restrict access to only those “friends” they want to share information with); Social Media Case Law and the Expectation of Privacy: US v. Meregildo, supra note 69 (mentioning that Facebook users can control privacy settings and determine who sees their posts and other information); Sabin, supra note 46, at 708 (explaining that social media users can limit access to their Facebook profile to specific individuals or groups). See also Miller, supra note 2, at 403 (explaining that Twitter allows the user to set their profile to “public” or “private” and if the user does not limit the account to a more private setting, public posts on Twitter may be viewed by anyone). In addition, some social media platforms allow users to create pseudonymous accounts. Id. 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. Id. While some anonymous social media users might hide for nefarious reasons, others use pseudonyms for protecting reputations or personal safety. Id. at 404.

113 See Miller, supra note 2, at 413 (arguing that the use of the pseudonymous handle on social media platforms creates a likely actual expectation of privacy). Someone who creates a pseudonymous account does so with an expectation that viewers will not know their identity. Id. In addition, much of the information that can be discovered by social media monitoring, such as location information or one’s online relationships status, is thought of as private. Id. It is likely that society would then recognize the expectation of privacy on social media as reasonable because if there was no expectation of privacy, it is unlikely many people would create pseudonymous accounts in the first place. Id.
antiquated and should be reworked to better fit modern society and protect an individuals’ privacy on social media.\textsuperscript{114}

\textbf{B. The Lack of Information on Social Media Monitoring Opens the Door to Discriminatory Pretexual Denials}

The State Department’s failure to disclose what constitutes a national security concern and what is considered grounds for denying a foreign national’s visa petition opens the door to arbitrary and abusive decision-making by adjudicating officers.\textsuperscript{115} Ultimately, the State Department can use information gathered from foreign nationals’ social media accounts to target individuals that the government disfavors due to attributes such as their ethnicity, religion, or political beliefs.\textsuperscript{116} Although the State Department has stated that the collection

\textsuperscript{114} See Gee, supra note 59, at 288 (arguing that the third-party doctrine is anachronistic in the age of surveillance). Ultimately, Fourth Amendment jurisprudence needs to be updated to afford more privacy protections against government surveillance. \textit{Id.} at 290. One idea is that “Fourth Amendment safeguards should apply whenever citizens convey personal information to a trusted third-party under promise of confidentiality.” \textit{Id.} at 301.

\textsuperscript{115} See Waheed, supra note 8 (explaining that “a program ostensibly designed to identify ‘national security concerns’ has been underway, apparently without basic standards or guidance as to what constitutes such a ‘concern.’”). \textit{See also} Handeyside, supra note 35 (emphasizing that the lack of published standards for how the government can scrutinize social media data inevitably leads to arbitrary and abusive decision-making by consular officers). \textit{See also} Rejection of DHS Proposal, supra note 39 (revealing that immigration officials enjoy broad discretion to adjudicate immigration benefits and do so behind closed doors); \textit{POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra} note 8 (arguing that collecting social media data for the purpose of vetting foreign nationals seems highly unlikely to contribute measurably to domestic safety and security, and more likely to have the effect of facilitating religious, ideological, or cultural screening). \textit{See also} Supporting Statement, supra note 7, at 15 (admitting that members of the public were concerned that the State Department’s social media monitoring was part of a larger endeavor with discriminatory motives). Over 572 commenters asked for specifics regarding what information contained in social media postings or pages may result in a denial. \textit{Id.} at 10.

\textsuperscript{116} See Supporting Statement, supra note 7, at 10 (arguing that the policy will allow State Department officials to restrict entry to the U.S. to only people whose views and opinions they agree with). \textit{See also} Stop Collecting Immigrants’ Social Media Data, supra note 5 (highlighting how irrelevant information collected on social media can be used to go after people the government disfavors by refusing them entry to the country or targeting them for investigation). \textit{See also} Social Media
of social media identifiers will not be used to deny visas solely “on the basis of race, religion, ethnicity, national origin, political views, gender, or sexual orientation,” officers are nevertheless given wide discretion to adjudicate applications with no safeguards in place to prevent pretextual denials. The large amount of sensitive information that can be gleaned from social media, along with the broad discretion given to adjudicating officers, allows an officer’s subjective bias to easily infect their decision-making and is a recipe for discriminatory and pretextual outcomes.

Surveillance, supra note 27 (explaining that when the government gains access to a growing collection of personal information extracted from social media accounts, they may use it to subject religious minorities and communities of color to enhanced vetting and surveillance); Social Media Monitoring, supra note 7 (noting that “[w]hile agents obviously must have some flexibility to make judgments, the breadth of discretion combined with weak safeguards opens the door for discrimination based on political or religious views.”).

117 See Supporting Statement, supra note 7, at 16 (stating that under the State Departments’ policy, visas may not be denied on the basis of race, religion, ethnicity, national origin, political views, gender, or sexual orientation). However, one topic of concern surrounding the policy is the lack of meaningful oversight mechanisms, such as periodic audits and reviews or a formal dispute resolution mechanism for affected foreign nationals. Id. at 10. See also Social Media Monitoring, supra note 7 (highlighting that the State Department’s claim that visas will not be denied based on a foreign national’s race, religion, ethnicity, national origin, political views, gender, or sexual orientation can be easily circumvented). “[A] social media post revealing an applicant’s religious or political affiliation may not alone justify denial, but other information in his or her file could easily be used as a pretext, particularly given the broad discretion exercised by consular officials.” Id. See also Rejection of DHS Proposal, supra note 39 (explaining that while the State Department’s policy prohibits officials from considering certain attributes to deny visas, officials enjoy broad discretion to adjudicate immigration benefits and do so behind closed doors). See POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (noting how officers are in a position to exercise enormous, unchecked discretion when it comes to assessing foreign nationals’ suitability to enter the country).

118 See Rejection of DHS Proposal, supra note 39 (stating that “social media offers a flood of sensitive information about a person that would not be apparent from an immigration benefit application and is irrelevant to what they are being screened for.”). This amount of information, along with the broad discretion given to officers, allows for their subjective bias to infect decision-making and drive discriminatory
In addition, it is likely no coincidence that the State Department’s social media identifier registration requirement arose during the Trump administration’s Muslim ban and other “extreme vetting” initiatives. In fact, both the State Department’s social media monitoring policy, and the now-rescinded DHS proposal were preceded by Trump officials’ statements that social media screening was intended to facilitate vetting aimed at Muslims. Therefore, the State Department’s policy clearly represents the remnants of the Trump administration’s oppressive immigration policies and has discriminatory roots and objectives that foster pretextual denials.

C. Social Media Monitoring is Overall an Ineffective and Unnecessary Vetting Measure

The State Department’s collection of social media identifiers from visa applicants is both an unnecessary as well as ineffective method of outcomes. Id. See also Supporting Statement, supra note 7, at 10 (commenting that “[i]f this program is to be implemented at all, meaningful oversight mechanisms should be built into it, including periodic audits and reviews as well as a formal dispute resolution mechanism for affected persons.”).

See Social Media Surveillance, supra note 27 (indicating that the Trump administration is using social media surveillance of foreign nationals as a tool to keep particular visitors, especially Muslims, out of the U.S.). See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (arguing that the history of U.S. vetting procedures suggests an intent to make national origin and religious-based distinctions among applicants, with a focus on Muslims).

See also Rejection of DHS Proposal, supra note 39 (revealing that when rejecting the DHS’s proposal to collect social media identifiers, OIRA mentioned that the Muslim ban, which ordered the DHS’s proposal, had been repealed); Biden Administration Tells Court It Plans to Keep Trump-Era Social Media Vetting Policy for Visa Applicants, supra note 66 (highlighting that the White House rejected a practically identical proposal from the DHS to collect social media handles on its travel and immigration forms, noting that its usefulness had not been demonstrated and that the Muslim ban—the basis for it—had been repealed). See also Stop Collecting Immigrants’ Social Media Data, supra note 5 (finding that when former President Trump’s Muslim ban was struck down by federal courts, the State Department imposed additional vetting measures that just happened to cover about the same number of people as the ban).

See also Rejection of DHS Proposal, supra note 39 (emphasizing that the genesis of the State Department’s dragnet collection of social media identifiers is ripe for intentional, systematic profiling). See also Diakun, supra note 62 (commenting that the State Department’s policy—the vestige of former President Trump’s racist and oppressive immigration policies—should share the same fate as the executive order that gave rise to it).
vetting foreign nationals. The U.S. government has defended the social media monitoring policy as a vital means of protecting the country’s national security and an important check on a foreign national’s admissibility, yet has failed to explain with any specificity why it needs to conduct such extensive social media surveillance.\textsuperscript{123}

\textsuperscript{122} See Lau, supra note 6 (arguing that “while the government has justified its expansion [of social media monitoring programs] in the name of national security, there is little indication that these programs – or the algorithms that sometimes power them – are effective in achieving their stated goals.”). It is difficult to interpret what’s in social media messages and connect them to actual threats. \textit{Id. See also} Campbell, supra note 29, at 528 (revealing how data does not show that social media data collection has effectively prevented any national security threats or denied admissions to any dangerous peoples). In addition, there is no evidence that social media collection programs prevent any dangerous immigrants from entering the United States. \textit{Id.}

\textsuperscript{123} See Powell, supra note 63 (providing justifications for why the State Department would look through social media accounts: national security, inadmissibility, and fraud). The Government argues that they are looking for any obvious red flags that might indicate the immigrant could be a national security threat or otherwise burden law enforcement. \textit{Id.} In addition, social media allows the Government to check for clues that might indicate an immigrant was inadmissible to the United States for another reason and to check for any instances of fraud or misrepresentation in the application. \textit{Id. See also Privacy Impact Assessment, supra note 3} (explaining that social media can provide positive, confirmatory information to verify identity and support a foreign national’s immigration request, and it can also be used to identify potential deception, fraud, or previously unidentified national security or law enforcement concerns). \textit{See also} Bischof, supra note 7 (presenting the State Department’s argument that social media can be a major forum for terrorist sentiment and activity and that reviewing foreign nationals’ social media content will be a vital tool to screen out terrorists, public safety threats, and other dangerous individuals from gaining immigration benefits and setting foot on U.S.). \textit{But see} Glenn, supra note 10 (highlighting that “[t]he government hasn’t explained with any specificity why it needs to conduct social media surveillance—it’s just gestured abstractly at national security and the need to adjudicate visa applications.”). When the rights of individuals to speak freely online and the rights of U.S. citizens and residents to hear that speech are at stake, a much closer examination of the government’s interests and much more serious consideration of the First Amendment implications is needed. \textit{Id. See also} Stop Collecting Immigrants’ Social Media Data, supra note 5 (arguing that despite the government’s claims of threats to national security, there is scant payoff). “Empirical research shows that the likelihood of getting killed in a terrorist attack by an immigrant or visitor to [the U.S.] is vanishingly small.” \textit{Id. See also} POGO
Regardless, it is highly unlikely that the monitoring of foreign nationals’ social media will assist the government in uncovering potential terrorists applying for visas or other threats to the country’s national security. While social media can provide a great deal of information about an individual, many social media posts and interactions are subject to misinterpretation. For example, a British citizen was denied entry into the U.S. when DHS agents “misinterpreted his post on Twitter that he was going to ‘destroy America’ – slang for partying – and ‘dig up Marilyn Monroe’s grave’ – a joking reference to a television show.” The difficulties of interpreting a foreign national’s social media posts are exacerbated when the language used in the posting is not English or when the

_Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8_ (characterizing national security benefits as speculative).

_124_ See _POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8_ (revealing that the number of vetting failures that have allowed foreign nationals to commit terrorist attacks on U.S. soil is minuscule). The government assumes that the investigation of foreign national’s social media information will assist the State Department in uncovering potential terrorists applying for visas, however, this seems unlikely. _Id._  _See also_ _Supporting Statement, supra note 7, at 5_ (arguing that there is no evidence that human review or any algorithmic profiling rule sets will have any actual utility for predicting which individuals will engage in extremely rare acts of terrorism, regardless of the biographic data they analyze). _See also Stop Collecting Immigrants’ Social Media Data, supra note 5_ (disclosing that “[e]mpirical research shows that the likelihood of getting killed in a terrorist attack by an immigrant or visitor to this country is vanishingly small.”).

_125_ _Stop Collecting Immigrants’ Social Media Data, supra note 5_ (explaining that posts and tweets are often unreliable, as online communications often consist of jokes, shorthand speech, and cultural references that are hard for others to interpret); _CDT Complaint, supra note 77, at 2_ (highlighting that “[c]ommunication on social media is highly susceptible to misinterpretation because it is, like most human interaction, idiosyncratic.”). _See also Rejection of DHS Proposal, supra note 39_ (emphasizing that communication on social media can easily be misinterpreted as they are often highly context-specific and riddled with slang and jokes). Communications in non-verbal form that do not have universally accepted meanings are also subject to misinterpretation. _Id._ For example, it can be questionable whether a “retweet” on Twitter signals endorsement. _Id._ _See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8_ (noting that “problems of interpretation – which manifest in both manual and computerized review… – are guaranteed to plague any review of social media postings.”).

_126_ See _POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8_ (providing examples of government agents misinterpreting foreign national’s social media postings). “[G]overnment agents and courts have erroneously interpreted tweets repeating American rap lyrics as threatening messages in several court cases, including high-stakes national security matters.” _Id._
posting contains slang. In addition, computerized review of an individual’s social media – through the use of various algorithms – has proven even worse than manual review at accurately deciphering and understanding social media posts.

The State Department themselves has even alluded to the fact that their policies are not sufficiently effective. When questioned

127 See id. (admitting that even greater difficulties of interpreting social media posts are inevitable if the language used is not English). See also CDT Complaint, supra note 77, at 2 (highlighting that foreign nationals’ social media content may often contain foreign languages, which further complicates an analysis of their online posts and activity); Social Media Monitoring, supra note 7 (explaining that to accurately review social media data, government personnel must be able to understand more than 7,000 languages and the cultural norms of 193 countries). See also Stop Collecting Immigrants’ Social Media Data, supra note 5 (stating that the accuracy of social media interpretation “takes a nose-dive when the speech being analyzed is not standard English.”). In one instance, “the post ‘Bored af den my phone finna die!!!!’ was flagged by an algorithm as Danish with 99.9 percent confidence.” Id. See also Supporting Statement, supra note 7, at 5 (commenting that “[e]ven the most basic machine-based translation tools do not operate with sufficient accuracy to generate reliable translations, much less inferences based on those translations.”). Most commercially available natural language processing tools will likely misinterpret non-English text. Id.

128 See Stop Collecting Immigrants’ Social Media Data, supra note 5 (explaining that the government can use algorithms to help with the large volume of social media information for review, but that these algorithms simply cannot make the judgment calls required when reviewing this type of information). In addition, computers are even worse than humans in making sense of what is said on social media. Id. “Even the best natural language processing program generally achieves 70 percent to 75 percent accuracy, which means more than a quarter of posts would be misinterpreted.” Id. See also Social Media Surveillance, supra note 27 (revealing that agency employees manually review social media posts, but, according to some experts, the government also uses algorithmic tools). See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (quoting Homeland Security’s November 2017 report). “[D]ecisions based on automated social media content analysis risk further marginalizing and disproportionately censoring groups that already face discrimination”. Id. Ultimately, subjecting foreign national’s social media data to algorithmic analysis seems highly more likely to facilitate religious, ideological, or cultural screening, than to contribute measurably to domestic safety and security. Id.

129 See Decell & Panduranga, supra note 35 (noting that the government has failed in several attempts to prove social media screening’s effectiveness). See also
about issues with the effectiveness of their social media monitoring program, the State Department responded that they are “constantly working to find mechanisms to improve [their] screening processes.”

Notwithstanding the government’s recognition of the need for improvement of their policy, such invasive social media monitoring should not be utilized until effective mechanisms are in fact proven and implemented.

Along with being ineffective at identifying foreign nationals who pose national security threats or are otherwise inadmissible, the use of social media monitoring is altogether unnecessary. As an initial matter, there is scant evidence that foreign nationals present a serious terrorist risk to the U.S.

Supporting Statement, supra note 7, at 6 (admitting that the State Department is aware of the February 2017 Report cited by many critics and commentators and is constantly working to find mechanisms to improve their screening processes). See also DHS Inspector General Report, supra, note 23, at 2 (revealing that this 2017 Report established that the DHS had failed to establish mechanisms to measure the effectiveness of their pilot programs for social media screening).

See Supporting Statement, supra note 7, at 6 (mentioning that social media screening capabilities and effectiveness continue to evolve, and the State Department is working to improve the effectiveness of their screening processes).

See Social Media Monitoring, supra note 7 (highlighting that the consequences of allowing such unchecked and provenly ineffective social media monitoring policies to continue are too grave to ignore). See also Waheed, supra note 8 (insinuating that the government should not be “speeding ahead with social media surveillance, without regard for the concerns that have been raised” and the absence of any evidence that such policies can be carried out fairly and effectively).

See Waheed, supra note 8 (describing the State Department’s expanded social media collection as a solution in search of a problem). See also Diakun, supra note 62 (emphasizing that the State Department’s registration requirement is “entirely unnecessary, because, even absent the requirement, nothing will preclude consular officials from asking individual applicants for social media information when there are good reasons for doing so.”).

See Beauchamp, supra note 62 (finding that there’s precious little evidence that immigrants actually pose a serious terrorist risk to the U.S.). Research has found that almost 99% of all the deaths from immigrant attacks came from 9/11, and that other than that, fatal immigrant-linked terrorist attacks in the U.S. were vanishingly rare. Id. “The average likelihood of an American being killed in a terrorist attack in which any kind of immigrant participated in any given year is one in 3.6 million — even including the 9/11 deaths.” Id. See also POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (finding that empirical evidence shows that the risk of an attack on U.S. soil perpetrated by a foreign person who has been improperly vetted is infinitesimal).
on their social media accounts, it is unlikely that they would be honest in disclosing their social media identifiers to the State Department. Finally, the State Department’s social media registration policy is unnecessary because, even without the policy, government officials still have the authority to ask certain foreign nationals for their social media information when the request is justified. In fact, the State Department previously used Form DS-5535 (Supplemental Questions for Visa Applicants) to request social media identifiers for the last five years for those immigrant and nonimmigrant visa applicants “who [were] determined to warrant additional scrutiny in connection with terrorism or other national security-related visa ineligibilities.”

134 See POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (explaining that it is “doubtful that an individual who promotes terrorism online will disclose information about the social media profile he is using to do so, or will retain postings that might get flagged as problematic.”).  
135 See POGO Urges DHS to Abandon Problematic Social Media Collection Plan, supra note 8 (emphasizing that the U.S. has one of the world’s most thorough visa vetting systems that is built to identify national security threats). “According to a federal court of appeals: ‘There is no finding that present vetting standards are inadequate, and no finding that absent the improved vetting procedures there likely will be harm to our national interests.’” Id. See also Diakun, supra note 62 (noting that the State Department’s social media registration requirement is entirely unnecessary, because, even absent the requirement, nothing will preclude consular officials from asking individual applicants for social media information when there are good reasons for doing so); Glenn, supra note 10 (admitting that if the State Department has good cause to look into a particular applicant further, it can do that, however, it shouldn’t be collecting social media handles without an individualized need).  
136 See Butler, supra note 15 (explaining that the DS-5535 requires social media platforms and identifiers for the last five years as well as 15 years of travel history, addresses and employment, and identification of family members). See also 2017 Notice, supra note 27, at 20957 (explaining that the State Department used Form DS-5535 to request social media platforms and identifiers from a subset of visa applicants worldwide, in order to more rigorously evaluate applicants for terrorism or other national security-related visa ineligibilities). Form DS-5535 is requested from immigrant and nonimmigrant visa applicants who have been determined to warrant additional scrutiny in connection with terrorism or other national security-related visa ineligibilities. Id. See also 30 Day Notice, supra note 69, at 8475 (explaining that while the State Department previously required applicants completing the DS-5535 to provide their social media platforms and identifiers used
Ultimately, the non-negotiable condition that approximately 14.7 million visa applicants per year be required to provide their social media handles is unnecessary and needlessly intrusive, and the seizure of such information should require reasonable suspicion of involvement in harmful activity or fraudulent conduct.\textsuperscript{137}

V. Conclusion

The U.S. government has a vital responsibility and national security interest in vetting all foreign nationals who seek to enter the country. While requests for foreign nationals’ contact information, family member and addresses history, and other biographical information are necessary to conduct such vetting, the collection of foreign nationals’ social media identifiers used during the past five years from the date of the application is overly intrusive and detrimental. It is evident from the proven ineffectiveness and harmful implications on individuals’ Constitutional rights that the government needs to reassess and abandon the unjustified use of social media monitoring in immigration matters. If, however, social media monitoring practices are to continue, the DHS and State Department should be required to fully disclose to the public how they monitor and

\textsuperscript{137} See Timeline, supra note 20 (noting that the State Department’s social media collection policy asks all visa applicants – an estimated 14.7 million people per year – to provide social media identifiers); Doc Society v. Blinken, supra note 36 (emphasizing that the State Department’s registration requirement, which affects about 15 million people a year, was a major expansion of the government’s probing into the social media activity of immigrants to the U.S.). See also Glenn, supra note 10 (arguing that no one has challenged the government’s authority to conduct suspicion-based social media surveillance, but they have challenged the State Department’s dragnet social media surveillance of all visa applicants); Supporting Statement, supra note 7, at 6 (arguing that the seizure of five years of one’s social media handles should require “reasonable suspicion of involvement of the individual in a crime, rather than being a non-negotiable condition for the granting of a visa.”). See also Iovino, supra note 81 (arguing that “[e]ven though social media profiles are public, that doesn’t mean the government should be monitoring that information in a dragnet fashion without any suspicion of wrongdoing.”). See also Everything You Need to Know About the New DHS Social Media Policy, supra note 1 (suggesting that because the State Department’s policy impacts such a large number of applicants, it will create further delays in an already backlogged immigration system).
retain social media data and use this information when adjudicating U.S. immigration petitions. In addition, the government should be required to implement competent oversight mechanisms, such as periodic audits and reviews, to minimize discriminatory and unjustified application denials and ultimately ensure foreign nationals have a fair and reasonable opportunity to enter or remain in the U.S.