THE CENTER ON RACE INEQUALITY & THE LAW
NYU SCHOOL OF LAW

October 16, 2025

Department of Homeland Security; U.S. Citizenship and Immigration Services
John R. Pfirrmann-Powell
Telephone: (240) 721-3000

Re: Department of Homeland Security; U.S. Citizenship and Immigration Services [OMB Control Number 1615-NEW]

Dear Mr. Pfirrmann-Powell,

The Center on Race, Inequality, and the Law at NYU School of Law uses research, advocacy, litigation, and public education to advance racial and social justice for all.[1] In keeping with that mission, we submit this comment in response to the Department of Homeland Security's ("DHS") proposed rule to allow generic clearance for the collection of social media identifier(s) on immigration forms.[2]

As an academic center that illuminates and challenges an array of American laws, policies, and practices that perpetuate racial oppression and injustice, we recognize the role immigration policies play in the shaping of the social and political composition of the United States. Throughout the United States' history, immigration has been a vehicle for the enrichment of the nation's cultural fabric, the reinvigoration of the labor force, and the strengthening of democratic values. To this end, the role of U.S. Citizenship and Immigration Services (the "USCIS") is to enhance the security and efficiency of administering immigration benefits. However, DHS' proposed collection of social media identifiers on immigration forms undermines USCIS' role because it fails to adequately improve national security screening and vetting, while detrimentally burdening the agency's resources. Further, the proposed collection

1This comment has been prepared by the Center on Race, Inequality, and the law at NYU School of Law, but does not purport to present the school's institutional views, if any.
2New Collection: Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms, 90 Fed. Reg. 11324 (October 16, 2025), https://www.federalregister.gov/documents/2025/09/16/2025-17816/agency-information-collection-activities-new-collection-generic-clearance-for-the-collection-of (hereafter "Collection Notice").

Center on Race, Inequality, and the Law
New York University School of Law
139 MacDougal Street, Fourth Floor
New York, NY 10012

chills freedom of speech, association, and privacy under the First Amendment, while enabling the unlawful mass surveillance of millions of people, with a disproportionate impact on historically marginalized communities and political dissidents. For these reasons, we urge DHS to withdraw its proposal.

The proposed rule – in particular the request to collect social media identifier(s) – raises three interrelated concerns that should compel DHS to withdraw it. First, the proposed collection contravenes freedom of speech, association, and privacy, as protected under the First Amendment. Second, the proposed collection has a disproportionate impact on political dissidents and historically marginalized communities. Finally, the proposed collection inadequately appreciates the risk of data breaches.

Given these concerns and the lack of sufficient mitigating factors, the implementation of the proposed rule unjustifiably places too many people in vulnerable positions as it pertains to their privacy and First Amendment freedoms. We respectfully request that DHS withdraw the proposed rule in light of these considerations.

The proposed collection of social media identifiers illegally subjects millions of people, including American citizens and non-citizens, to state-sponsored mass surveillance which has a chilling effect on the expression of political speech

Social media platforms have become integral parts of people's everyday lives. These platforms have increasingly become the primary way for people to document memories and events, connect with others, and express themselves. Despite the public nature of these platforms, the information that can be gleaned from a review of one's social media is quite comprehensive. As stated by the United States Supreme Court in *Riley v. California*, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labels with dates, locations, and descriptions."[3] In this vein, social media reviews can reveal cultural identifiers, professional affiliations, sexual identities, religious associations, and other discrete group memberships. Consequently, this information is far more expansive and personal than that which is revealed and necessary for immigration adjudication purposes.[4]

As categorized by DHS policies, the collection of social media identifiers falls under the category of sensitive personally identifiable information ("SPII"). This category requires

3*Riley v. California*, 573 U.S. 373, 393 (2014).

4*Carpenter v. U.S.,* 585 U.S. 296, 312 (2018) ("Moreover, the retrospective quality of data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection…the Government can now travel back in time to retrace a person's whereabouts").

additional privacy risk mitigation strategies, as the disclosure of this information could "result in substantial harm, embarrassment, inconvenience, or unfairness to an individual."[5] The consequences associated with disclosure of SPII in part explains why, as repeatedly affirmed by the Supreme Court, the right to anonymity is essential to the protection of First Amendment free speech.[6] It also explains the connection between surveillance and self-censorship.

As acknowledged by Justice Sotomayor, "[a]wareness that the Government may be watching chills associational and expressive freedoms."[7] The collection and inspection of social media identifiers as a requisite to immigration benefits infringes upon the privacy of visa applicants and those they associate with online. In response to this infringement, applicants, understandably concerned with the implications of their online activity on their immigration status, will necessarily change how and with whom they engage. This change may take many forms: limitations on the type of information shared, complete disengagement from online platforms, restrictions on interactions, and disassociation from individuals and online community group. Each of these methods constitutes some form of self-censorship.

Focusing on political speech, many people rely on the use of pseudonymous social media identifiers to express opinions on controversial political and social topics. These pseudonyms provide a shield for the user and their associates from retaliation by state or local actors, as well as their own communities. When access to immigration benefits is conditioned on the disclosure of social media identifiers, applicants find themselves between a rock and a hard place. They are forced to weigh their desire to speak out on important issues against the risk of negative immigration consequences that accompany refusal to provide the required information. Faced with this choice, applicants understandably choose to forgo traveling to the United States entirely or change their online behavior.

Adding to the chilling effect on political speech, aside from concerns about DHS' use and monitoring of the applicant's social media, the proposed collection would, on some forms, require the disclosure of the social media identifiers of an applicant's associate, whose

5See Privacy Office, Privacy at DHS: Protecting Personal Information FY25, DHS, October 2024, 3 https://www.dhs.gov/sites/default/files/2024-10/2024_1023_PrivacyatDHStranscript.pdf; and Privacy Office, Privacy Threshold Analysis Version Number: 04-2016, DHS, March 14, 2017, 3 https://www.brennancenter.org/sites/default/files/2022-03/PTA%202017%20SM%20as%20SPII.pdf (noting the collection of social media identifiers implicates "novel privacy risks").

6"Anonymity." n.d. EPIC – Electronic Privacy Information Center. https://epic.org/issues/democracy-free-speech/anonymity/ ("The Supreme Court has repeatedly affirmed that a right to anonymity lies in the First Amendment."

7*United States v. Jones,* 565 U.S. 400 (2012) (Sotomayor, J., concurring).

relationship may be relevant to the immigration benefit being sought.[8] This exponentially increases the scope of government surveillance, and correspondingly the amount of people, particularly American citizens, who will likely self-censor. Not only do applicants need to worry about what their personal social media accounts might portray, but also those associated with the applicant – whether intentionally or not – will likely be encouraged to assume a more muted posture.

As most of these forms evaluate connections between applicants and residents within the United States, the data of American citizens will necessarily be subject to the types of "rigorous vetting and screening" the proposed rule purports to achieve.[9] Out of fear of jeopardizing their relative's application, relatives of the applicant (and arguably friends of an applicant's relatives) will likely engage in some degree of self-censorship, thereby creating a chilling effect on speech that is felt both domestically and internationally.

Privacy expectations and the intrusive nature of the data collected raise additional concerns. As identified in *Carpenter v. U.S.,* "the retrospective quality of the data here gives [the agency] access to a category of information otherwise unknowable."[10] As the Court has consistently maintained, much of the underlying logics of privacy protection relate to a reasonable person's expectation of privacy.[11] Acknowledging limitations of surveillance prior to the digital age, the Court is guided by the prevailing expectation that "law enforcement agencies and others would not – and indeed, in the main, simply could not – secretly monitor and catalogue every single movement" of an individual for an extended period of time.[12] This expectation persists today and has been a justification for the Court's recognition of the enhanced capabilities of government surveillance.[13] To this end, social media data has been likened to location tracking and cell phone data, which the Supreme Court has afforded constitutional protections because they expose the type of "the time-stamped data [which] provides an intimate window into a person's life, revealing not only [one's] particular movements," but [one's] associations with others.[14] Necessarily, the expectations of privacy persist regardless of whether this information has been disclosed to the public at large through voluntary posting on social media.[15]

8Examples include form I-751 ("Petition to Remove Conditions on Residence"), form N-400 ("Application for Naturalization"), and form I-485("Application to Register Permanent Residence or Adjust Status").
9See Collection Notice.
10*Carpenter v. U.S.,* 585 U.S. at 312.
11*See, eg., Carpenter, Riley,* and *Jones.*
12*Carpenter,* 585 U.S. at 310.
13*Kyllo* v. *United States*, 533 U. S. 27, 34, (2001).
14*Carpenter,* 585 U.S. at 311.
15*Id.* at 307.

The proposed collection requires applicants to list all social media identifiers reaching back five years.[16] Recognizing the "immense storage capacity" of modern cell phone as a justification for requiring warrants before law enforcement can perform a search, the virtually limitless capacity of social media platforms informs the degree to which the proposed collection impinges on expectations of privacy. Through this surveillance, the government is able to see " a wealth of detail about [an applicant's] familial, political, professional, religious, and sexual associations."[17] Social media profiles "collect[] in one place many distinct types of information … that reveal much more in combination than any isolated record."[18] Regardless of whether DHS officials intentionally look for information relating to an applicant's associations and affiliations, the very fact that they have access to this information raises concerns of bias within the decision-making process and raises the risk of abuse if the information is shared and used for purposes beyond the proposed collection's intent.

The proposed collection has a disproportionate impact on political dissidents and historically marginalized communities.

Enacted in response to the Watergate and the Counterintelligence Program scandals, the Privacy Act is undergirded by the idea that "there must be limits upon what the Government can know about each of its citizens."[19] To this end, the Privacy Act protects against unwarranted intrusions into an individual's privacy. Particularly, the Privacy Act is concerned with safeguarding information that can be used to identify an individual. Arguably one of the most important features of the Privacy Act is the limitations it places on agency data sharing and storage. Pursuant to its purpose, limitations are placed on the use of 'matching programs'; automated systems that compare databases in order to link certain characteristics to a particular individual.[20]

In violation of the Privacy Act, existing DHS policies actively enable data sharing between local, state, and federal government agencies, heightening the concerns around the targeting of specific communities."[21] Given the scope of the proposed collection of information, data

16See, N400-021-INS-TOC-SocialMedia-FOReview-03052025 available at https://www.regulations.gov/document/USCIS-2025-0003-0036.
17*Jones*, 565 U.S. at 415 (Sotomayor concurrence).
18*Riley*, 573 U.S. at 394.
19"Overview of the Privacy Act: 2020 Edition." 2020. U.S. Department of Justice. October 14, 2020 https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction#LegHistory (Spoken by Judicial Chairman Senator Sam Ervin, the bill's principal sponsor).
205 U.S. Code §552a(a)(8).
21DHS, Privacy Act of 1974; System of Records https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records (existing DHS policies which actively enable data sharing with

collected by USCIS, though irrelevant to the immigration process, can be shared and used by another agency to target an individual. Data sharing of this sort ultimately enables the government to identify and group tenuously connected individuals to target those it deems opposed to its agenda.

The collection, storage, and dissemination of such broad amounts of personally identifiable information has disproportionately affected historically marginalized communities, political disfavored individuals, and their freedom to associate.[22] The United States has a long history of wielding national security as a justification for using broad surveillance discretion to identify and target politically unpopular groups. Focusing specifically on Black political activists, the expansion of state sponsored surveillance is intimately entangled with the history of Black liberation movements.[23] In the early 1900s, the Federal Bureau of Investigations (the "FBI") labeled activists such as Ida B. Wells and Marcus Garvey "race agitators" to justify their use of illegal monitoring tactics.[24] In the 1960s, through its Counterintelligence Program

"appropriate Federal, State, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, when DHS believes the information would assist in enforcing applicable civil or criminal laws.")

22*See generally*, "Guilty by Association: How Police Database Punish Black and Latinx Youth" S.T.O.P – the Surveillance Technology Oversight Project. September 5. 2023. https://www.stopspying.org/guilt-by-association (highlighting the ways law enforcement utilizes surveillance technology to disproportionately target and monitor Black and Latinx communities) (hereafter "S.T.O.P"); Additionally, the government has repeatedly abused its broad surveillance discretion to target those it deems politically disfavored. As underscored by recent cases such as those of Mahmoud Khalil, Rumrysa Ozturk, Mohsen Mahdawi, and Yunseo Chung, the Trump administration, through a slew of executive orders, has rendered opposition to current ideological narratives sufficient grounds for negative immigration consequences (The Associated Press, "ICE Arrests Palestinian Activists Who Helped Lead Columbia University Protests." NPR. March 10, 2025. https://www.npr.org/2025/03/10/g-s1-52923/immigration-agents-arrest-palestinian-activist-columbia-protests; Ana Ley, Sharon Otterman, and Anvee Bhutani, "He Wanted Peace in the Middle East. Ice Wants to Deport Him." *The New York Times*. April 17, 2025 https://www.nytimes.com/2025/04/16/nyregion/columbia-activist-mahdawi-ice-palestinian.html; Miranda Jeyaretnam, "These Are the Students Targeted by Trump's Immigration Enforcement over Campus Activism." *TIME*. March 17, 2025 https://time.com/7272060/international-students-targeted-trump-ice-detention-deport-campus-palestinian-activism/; The White House, "Additional Measures to Combat Anti-Semitism" The White House. January 29, 2025 https://www.whitehouse.gov/presidential-actions/2025/01/additional-measures-to-combat-anti-semitism/; The White House, "Restoring Truth And Sanity To American History" The White House. March 27, 2025 https://www.whitehouse.gov/presidential-actions/2025/03/restoring-truth-and-sanity-to-american-history/).

23Andrea Dennis, "Mass Surveillance and Black Legal History" American Constitution Society. February 18, 2020 https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history;"The Racist Past of Government Surveillance" ACLU of Maryland. September 15, 2020 https://www.aclu-md.org/news/racist-past-government-surveillance/.

24Andrea Dennis, "Mass Surveillance and Black Legal History" American Constitution Society. February 18, 2020

("COINTELPRO"), the FBI engaged in a series of covert and illegal investigations of activists and social movements it deemed to be a threat to national security. The stated goal of the program was to infiltrate "expose, disrupt, and neutralize".[25] Noteworthy targets of COINTELPRO include Dr. Martin Luther King Jr., Malcom X, and the Student Nonviolent Coordinating Committee ("SNCC").

An illustrative example of the government's tendency toward abuse of discretion is the legislative history behind the Foreign Intelligence Surveillance Act of 1978 (the "FISA"). In response to the public scandals surrounding the surveillance of Dr. Martin Luther King, Jr. and other domestic surveillance abuses, Congress created the Church Committee to investigate allegations of the United States' government spying on American citizens.[26] The Committee reported a widespread abuse of surveillance overreach that "was not the product of nefarious officers but rather of unchecked powers."[27]As described by Senator Walter Mondale's "eerily prescient statement", the concern that the National Security Agency (the "NSA") "could be used by President 'A' in the future to spy upon the American people, to chill and interrupt political dissent" was a motivating factor for the enactment of FISA and other privacy related safeguards.[28] Necessarily, as it relates to disproportionate impact, Congressional records explicitly acknowledge that "the many African-American activists who were targeted by intelligence agencies…serve as cautionary tales for the expanding surveillance state."[29]

This use of surveillance as a way to infiltrate and discredit political dissidents and monitor historically marginalized groups has persisted into the digital age as technological advances have expanded the scope of government data collection.[30] As seen across the United

https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history.

25"Federal Surveillance of African Americans" UNCW Library https://library.uncw.edu/eresources/federal_surveillance_african_americans.

26Dia Kayyali "The History of Surveillance and the Black Community". Electronic Frontier Foundation. February 13, 2014 https://www.eff.org/deeplinks/2014/02/history-surveillance-and-black-community; Cited in the Congressional House Record (October 23, 2017) https://www.govinfo.gov/content/pkg/CREC-2017-10-23/pdf/CREC-2017-10-23-pt1-PgH8066-2.pdf#page=1.

27Max Rerucha, "Legislative, executive, and Judicial Shaping of the Foreign Intelligence Surveillance Act (FISA) and the Need for a Cleared Federal Public Defender" DePaul Journal for Social Justice. Volume 11 Issue 1. (January 2018), 9 https://via.library.depaul.edu/cgi/viewcontent.cgi?article=1160&context=jsj.

28Dia Kayyali "The History of Surveillance and the Black Community". Electronic Frontier Foundation. February 13, 2014 https://www.eff.org/deeplinks/2014/02/history-surveillance-and-black-community.

29*Id.*

30Andrea Dennis, "Mass Surveillance and Black Legal History" American Constitution Society. February 18, 2020 https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history.

("If anything today is different from historical Black experiences with government surveillance, it's that 21st century technology advances have made the practice far easier and more widespread. What was once limited to human, street-level surveillance or wiretaps has expanded to include Black people's online activities. From social platforms such as Facebook, Twitter, and Instagram to content-sharing sites such as YouTube, SoundCloud, and

States, cities with gang databases have used the collection of personally identifiable information to disproportionately target Black and Latinx communities.[31] This is underscored by the demographic make-up these databases—Black and Latinx youth account for 99% of those included in NYPD's database, and over 96% of the people in Chicago's database.[32] Many of these individuals have been added to these databases "under no individual suspicion of a crime" simply because they fit the profile of those believed to engage in criminal activity.[33] And as a consequence of the data sharing between local, state, and federal agencies, "any baseless accusation in one police department's record can really make the rounds – all the way up to federal agencies and across the nation to agencies in other states."[34]

Consequently, this collection of information has serious implications for one's freedom to associate. The disclosure of one's social media profile, as required pursuant to DHS' proposed rule, effectively amounts to the disclosure of one's associates. A review of one's social media necessarily reveals all those who a user – through likes, shares, or comments – has engaged with, and in turn those who have engaged with the user. These engagements capture a wide range of connections, ranging from close family and friends to acquaintances and even strangers. Because attempts to derive inferences about people's actions and associations from social media activity are fraught with highly contextualized norms and communication conventions that make it extremely difficult to objectively interpret, even the most attenuated interactions between users could link them as associates.[35]

These determinations of associations, though often overemphasized and inaccurate, carry serious consequences for both applicants and those with whom they are believed to associate. Applicants and their associates can be denied a benefit "simply by suspicion or association" rather than as a result of actual wrongdoing.[36] For example, in 2019, Ismail Ajjawi,

Spotify, law enforcement can watch and listen to whole communities, all from the comfort of their removed, secure offices.")

31 S.T.O.P at 1 ("under stop-and-frisk, the NYPD targeted young Black and Latinx men under no individual suspicion of a crime because they fit the department's racist profile of who engages in criminal activity…it has also increasingly relied on dystopian 'gang' databases to track the same Black and Latinx New Yorkers based on who they know and where they live…").

32 *Id.* at 6.

33 *Id.* at 1.

34 *Id.* at 3.

35 *Id.* at 4 ("Individuals are routinely added to gang databases for the flimsiest reasons. In New York City, the NYPD has added people in its gang database for being Facebook friends with an accused gang member or for wishing them 'Happy Birthday").

36 Emmanuel Felton, "Gang Databases Are a Life Sentence for Black and Latino Communities" Pacific Standard. March 15, 2018. https://perma.cc/7XGC-JHNK; Philip Marcelo, "Gang Databases Made Up Mostly of Young Black, Latino Men" Associated Press. July 30, 2019. https://perma.cc/3AZ2-59K5 ("Central American youths are being wrongly listed as active gang members "based on nothing more than the clothing they are seen in and the

a Palestinian student, is said to have been denied entry after custom agents questioned him about his friend's social media activity.[37] When questioned by an immigration agent, Ajjawi was told that "people posting political points of view that oppose the U.S. [were] on [his] friend list."[38] Similarly, in a recent cable to consular officers, the State Department has directed the review of student visa applicants' online presence for "any indications of hostility towards the citizens, culture, government, institutions or founding principles of the United States."[39] The lack of specificity of "indications" and what constitutes "hostility" opens the door for the targeting of anyone remotely connected to someone who disagrees with the administration on virtually any issue. This type of broad discretion obfuscates transparency and denies any form of meaningful accountability. Without explicit guidelines on what information is being collected and against which criteria it is being analyzed, the sharing of unreliable data – whether intentional or accidental –has the potential to cause inordinate harm to both applicants and those with whom they are believed to associate.

As encapsulated by the concerns of civil rights activists, the reality of this broad discretion is a guilt by association regime whereby "both the expansiveness and secret nature of [these] databases means that communities of color must live in fear."[40]

The proposed collection inadequately appreciates the intolerably high risk of data breaches.

Given the nature of the information being collected, the trend of weakened infrastructural oversight, and DHS failures to comply with internal privacy guidelines, there is a serious lack of appreciation for the very real risk of data breaches. This risk is intolerably high as there is no evidence that the screening of social media is a useful tool for national security or immigration vetting.

classmates they are seen with," and that's led some to be deported, the organizations say in their lawsuit, citing the cases of three Central American youths facing deportation based largely on their status on the gang database… One 24-year-old native of El Salvador nearly deported last year over his alleged gang involvement said he was a victim of harassment and bullying by Bloods members as a youth and was never an MS-13 member, as police claim.")

37Karen Zraick and Mihir Zaveri, "Harvard Student Says He Was Barred From U.S. Over His Friends' Social Media Posts," *New York Times.* August 27, 2019. https://www.nytimes.com/2019/08/27/us/harvard-student-ismail-ajjawi.html.

38*Id.*

39Nahal Toosi and Eric Bazail-Eimil, "State Department Unveils Social Media Screening Rules for All Student Visa Applicants," Politico. June 18, 2025. https://www.politico.com/news/2025/06/18/social-media-screening-student-visas-00413160.

40Emmanuel Felton, "Gang Databases Are a Life Sentence for Black and Latino Communities," Pacific Standard, March 15, 2018, https://perma.cc/7XGC-JHNK.

Consistent with the current administration's efforts to undermine internal security infrastructure and oversight accountability mechanisms, there has been a significant reduction of the Cybersecurity and Infrastructure Security Agency (CISA) and DHS' Office for Civil Rights and Civil Liberties.[41]

CISA is the agency primarily responsible for monitoring and protecting critical government infrastructure. As stated by Michael Daniel, the president and CEO of the Cyber Threat Alliance, these "reductions to CISA will weaken U.S. cybersecurity at a time when cyber threats are only increasing."[42] News of national data breaches are hardly uncommon. As recent last month, an internal DHS memo obtained through FOIA revealed a two month long breach whereby one of its platforms which housed the sensitive but unclassified intelligence information of agencies such as DHS, the National Counterterrorism Center, the FBI, and local law enforcement groups, was misconfigured to grant access to 'everyone.'[43] As a result of the breach, thousands of unauthorized users had access to information regarding law enforcement investigation leads and critical national security information. Despite DHS' characterization of the breach as "minimal to low impact", the exclusion of any analysis of the amount of personally identifiable information exposure, undermines this assessment. Given that social media identifiers are SPII, the risks associated with unauthorized exposure places millions of people, including American citizens, in very vulnerable positions.

Similarly, the reduction of the Office for Civil Rights and Liberties by the Department of Government Efficiency ("DOGE") effectively marked the end of internal DHS oversight.[44] The office had been tasked with ensuring DHS compliance with civil rights requirements and investigating claims of abuses and violations, so its closure is particularly troubling in light of DHS' failure to comply with its own internal measures meant to safeguard its collection and management of private information. Pursuant to its purpose, the Privacy Act implemented the

41David Jones, "Trump Administration Under Scrutiny as It Puts Major Round of CISA Cuts on the Table." Cybersecurity Dive. April 7, 2025. https://www.cybersecuritydive.com/news/trump-scrutiny-cisa-cuts/744619/; J. David McSwane and Hannah Allam, "They Don't Care About Civil Rights; Trump's Shuttering of DHS Oversight Arm Freezes 600 Cases, Imperils Human Rights" ProPublica. April 8, 2025. https://www.propublica.org/article/homeland-security-crcl-civil-rights-immigration-border-patrol-trump-kristi-noem

42David Jones, "Trump Administration Under Scrutiny as It Puts Major Round of CISA Cuts on the Table." Cybersecurity Dive. April 7, 2025. https://www.cybersecuritydive.com/news/trump-scrutiny-cisa-cuts/744619/.

43Andy Greenberg, "A DHS Data Hub Exposed Sensitive Intel to Thousands of Unauthorized Users" Wired. September 16, 2025. https://www.wired.com/story/a-dhs-data-hub-exposed-sensitive-intel-to-thousands-of-unauthorized-users/.

44J. David McSwane and Hannah Allam, "They Don't Care About Civil Rights; Trump's Shuttering of DHS Oversight Arm Freezes 600 Cases, Imperils Human Rights" ProPublica. April 8, 2025. https://www.propublica.org/article/homeland-security-crcl-civil-rights-immigration-border-patrol-trump-kristi-noem.

Fair Information Practice Principles ("FIPP") which represent widely accepted principles that outline the guidelines for federal agencies' collection and retention of personal information. While FIPPS are not necessarily requirements that all agencies must follow, DHS' Privacy Office formally adopted the FIPPs as the framework for is all its privacy policies and holds that these principles "must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status."[45] With heightened attention to the principles of use limitation and data minimization, the inability to place adequate boundaries on the scope of data collection and data sharing with other agencies raises concerns about the agency's willingness to comply with polices it has adopted for itself. These concerns provide sufficient reason to worry that the information collected by DHS will undermine individual privacy, unjustifiably expand the scope of government surveillance, and place millions of people at risk of unauthorized disclosure of highly sensitive personally identifiable information.

Further, as evidenced by its failure to satisfy the requirements of the Paper Reduction Act of 1995 ("the PRA"), the risk of data breaches is risk is intolerably high as the proposed collection fails to demonstrate both the necessity of the collection and the practical utility of social media screenings in the performance of USCIS' functions. This failure is underscored by DHS' well-documented knowledge that this type of collection insufficiently enhances the screening and vetting process, while detrimentally increasing the resource burden on the agency.

The stated purpose of the PRA is to "reduce, minimize and control burdens and maximize the practical utility and public benefit of the information created, collected, disclosed, maintained, used, shared and disseminated by or for the Federal government."[46] The PRA authorizes the "promulgat[ion] of rules, regulations, or procedures necessary" to achieve this purpose. Practical utility refers to "the actual, not merely the theoretical or potential, usefulness of information to or for an agency, taking into account its accuracy, validity, adequacy, and reliability, and the agency's ability to process the information it collects… in a useful and timely fashion."[47]

Thus, pursuant to the PRA, federal regulations require: (1) a showing of necessity whereby the proposed collection of information is justified as essential to USCIS' lawful function, (2) an explanation of the demonstrated usefulness of said collection to USCIS decision

45See, Privacy Policy Guidance Memorandum, Homeland Security, December 29, 2008, 3
https://www.dhs.gov/sites/default/files/2024-01/Fair%20Information%20Principles_12_2008.pdf
465 C.F.R. §1320.1 (2025)
475 C.F.R. §1320.3(1) (2025)

making process, or (3) a description of the way the collected information would alleviate the agency's burden. Here, as detailed below, DHS has failed to meet any of the requirements.

A. *The proposed collection of social media identifiers is not necessary for the proper performance for the functions of USCIS.*

According to the notice: "This collection of information is necessary to comply with section 2 of the E.O. establishing enhanced screening and vetting standards and procedures enabling USCIS to assess an alien's eligibility to receive an immigration-related benefit from USCIS."[48] While compliance with an executive order may provide a background explanation for the agency's choice of action, this does not supersede existing statutory requirements of the PRA. It is the PRA, not the executive order, that regulates and authorizes the collection of data for immigration-related benefits. Therefore, the promulgation of rules and procedures pertaining to data collection must be directly linked to the necessity of the agency function action – here, USCIS' vetting and screening of applicants – to satisfy this requirement of the PRA.

DHS, through its request for review and clearance under the PRA, acknowledges the need for a justification but nonetheless provides no explanation of how the proposed collection is necessary to USCIS functioning. Rather, there is a glaring omission of any discussion pertaining to the need for this information, any existing deficiencies in the proper performance of the functions of USCIS that could be corrected by this collection, or how the information collected will be used. Without this discussion, the broad collection of social media identifiers cannot be said to be necessary for USCIS performance.

B. *The proposed collection of information lacks practical utility as it fails to consider "[the information's] accuracy, validity, adequacy, and reliability, and the agency's ability to process the information it collects…in a useful and timely fashion"*[49]

In April 2025, the Office of Management and Budget (the "OMB") rejected a similar proposal by DHS for generic clearance to collect social media information on immigration and travel applications.[50] The request was rejected on the grounds that "the agency [did] not

48 See Collection Notice.

49 5 C.F.R. §1320.3(1) (2025)

50 Office of Information and Regulatory Affairs, Office of Management and Budget (hereinafter OMB), "OIRA Conclusion re Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms," April 2, 2021, https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202007-1601-001.

adequately demonst[rate] the practical utility of collecting this information."[51] Similar to the April request, the current proposal fails to demonstrate practical utility as it provides no evidence to suggest that social media surveillance is an accurate or reliable tool for the type of enhanced screening and vetting the data collection is intended to achieve.

DHS has known for close to a decade that social media monitoring adds no value to the immigration screening and vetting process. In a 2016 USCIS Presidential Transition report, a DHS pilot program designed to use social media to vet refugees and applicants requesting an adjustment of status found that "the information in the accounts did not yield clear, articulable links to national security concerns, even for those applicants who were found to pose a potential national security threat based on other security screening results."[52] Similarly, in 2021, through FOIA litigation, the Knight Institute was able to obtain documentation from the Office of the Director of National Intelligence (the "ODNI") concerning the National Counterterrorism Center's assessment of the ineffectiveness of reviewing social media in the screening process. The emails obtained explicitly state that the incorporation of social media identifiers to vet applicants had "very little impact on improving the screening accuracy of relevant systems."[53]

As it relates to the practical utility requirement under the PRA, the request for this type of vetting despite DHS' continued acknowledgement of the ineffectiveness of social media in the vetting process demonstrates a failure to take into account the collection's "accuracy, validity, and reliability."[54] DHS' actions reflect not just a failure to account for these measures, but an active attempt to pursue collection of this information in spite of its ineffectiveness. As reflected in the 2021 report, there was a proactive attempt by the participants on the email chain to obfuscate the public disclosure of these findings. In response to an ODNI participant's expression of concern that "while the answer is appropriate that there is little value in [screening and vetting]…I would hate to see this impact the [United States Government]'s ability in the future to collect and use", a Director in the Intelligence Community states "if you could recraft the language that would be fantastic."[55] This evidence of past intentional concealment suggests that this proposed collection should be viewed as a means to a different end. Adopting the language of the ODNI participant, the stated goal of enhanced vetting and screening procedures seems to be a guise behind which DHS attempts to achieve some unrevealed "tertiary affects" associated with the collection of this highly sensitive data.

51 *Id.*
52 "USCIS Presidential Transition Records," DHS, December 12, 2016, 199.
53 See Office of the Director of National Intellifgence, ODNI, April 8-9, 2021 ODNI Email Chain https://knightcolumbia.org/documents/vr3kqowufe.
54 5 C.F.R. §1320.3(1) (2025).
55 *Id.*

C. *Use of the proposed collection of information increases, rather than minimizes, the burden on USCIS.*

Even if the collection of social media identifiers could be shown to improve the vetting process, DHS does not have the resources to handle the burden imposed by the collection and incorporation of this data. Despite the lack of demonstrated value, the collection and review of the requested social media information is onerous, time-consuming, and costly. According to the 2016 DHS transition memo, "the process of social media screening and vetting necessitates a labor intensive, manual review" and even if such screening can definitively be tied to an individual with a pending immigration benefit, the "authenticity, veracity, social context, and whether the content evinces indicators of fraud, public safety, or national security concern are often difficult to determine with any level of certainty."[56] The report goes on to say that "having [personnel] dedicated to mass social media screening diverts them away from conducting the more targeted enhanced vetting they are well trained and equipped to do."[57]

Reviewing an attempt to mitigate the onerous nature of social media surveillance, a 2017 report by the DHS Office of the Inspector General revealed that in a USCIS and Immigration and Customs Enforcement ("ICE") pilot program that screened social media profiles to assess whether the accounts were linked to "derogatory" social media information that could affect an applicant's eligibility for either benefits or admissibility, "the tool was not a viable option for automated social media screening."[58] Instead, the program found that manual review of accounts was more effective.[59]

Thus, given the nature of the information being collected, the trend of weakened infrastructural oversight, and DHS failures to comply with internal privacy guidelines, there is a serious lack of appreciation for the very real risk of data breaches. This risk is intolerably high as there is no evidence that the screening of social media is a useful tool for national security or immigration vetting. These factors, coupled with the burdens to freedom of association and

56"USCIS Presidential Transition Records," DHS, December 12, 2016, 201.
57*Id.* at 202.
58Office of Inspector General (hereinafter OIG), DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted), February 27, 2017, 3 ,https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.
59As recent as January 2025, DHS's Office of Inspector General released an audit of DHS development and use of artificial intelligence to minimize the burden of the collection and use of social media information, which found that DHS lacks the adequate governing infrastructure for responsible AI usage. Setting aside concerning findings regarding the lack of protections for civil rights and liberties, despite establishing an "AI strategy to guide enterprise-wide AI goals and objectives…it did not effectively execute the strategy…" (Joseph V. Cuffari, OIG, OIG-25-10: Final Report: DHS Has Taken Steps to Develop and Govern Artificial Intelligence, But More Action is Needed to Ensure Appropriate Use, DHS, January 30, 2025 https://www.oig.dhs.gov/sites/default/files/assets/2025-02/OIG-25-10-Jan25.pdf).

privacy, weigh against the adoptions of the proposed rule.

Conclusion

We respectfully ask that DHS withdraw the proposed collection requested. We hope our comment is taken into consideration.