

Office of Management and Budget

October 16, 2025

Re: “Agency Information Collection Activities; New Collection: Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms [OMB Control Number 1615-NEW, Docket ID USCIS-2025-0003]”

To Whom It May Concern:

We write to reiterate and expand upon our opposition to the proposed information collection identified by Office of Management and Budget (OMB) Control Number 1615-NEW and Docket ID USCIS-2025-0003, submitted by the Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS).<sup>1</sup>

DHS proposes to collect social media identifiers from more than three million people applying for immigration-related benefits each year, along with—under some circumstances—those of their minor children, spouses and former spouses, and parents and stepparents.<sup>2</sup> The proposal states that this collection is necessary for “enhanced identity verification, vetting and national security screening, and inspection.” Many of the people whose social media identifiers DHS proposes to collect are U.S. citizens and legal permanent residents, or individuals who otherwise have legal status and are physically present in the United States.<sup>3</sup>

---

<sup>1</sup> New Collection: Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms, 90 Fed. Reg. 44693 (September 16, 2025), <https://www.federalregister.gov/documents/2025/09/16/2025-17816/agency-information-collection-activities-new-collection-generic-clearance-for-the-collection-of> (hereinafter “Collection Notice”).

<sup>2</sup> See Collection Notice. The notice estimates that the total number of respondents will be 3,468,668. For examples of forms that would solicit social media handles from third parties, see, e.g., USCIS, USCIS-2025-0003-1242, DHS, September 17, 2025, <https://www.regulations.gov/document/USCIS-2025-0003-1242> (the proposed I-751 form), and USCIS, USCIS-2025-0003-1234, DHS, September 17, 2025, <https://www.regulations.gov/document/USCIS-2025-0003-1234> (the proposed I-829 form).

<sup>3</sup> Previously adopted collections of social media identifiers primarily targeted non-U.S. persons outside the United States. See, e.g., Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization, 81 Fed. Reg. 40892 (June 23, 2016), <https://www.federalregister.gov/documents/2016/06/23/2016-14848/agency-information-collection-activities-arrival-and-departure-record-forms-i-94-and-i-94w-and>; and Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 20956 (May 4, 2017), <https://www.federalregister.gov/documents/2017/05/04/2017-08975/notice-of-information-collection-under-omb-emergency-review-supplemental-questions-for-visa>. The current proposal, if approved, would involve collecting social media identifiers from U.S. citizens, lawful permanent residents, and other people lawfully residing in the U.S. See, e.g., the proposed revisions to forms I-751 and I-131. USCIS, USCIS-2025-0003-1250, DHS, September 17, 2025,

OMB should deny DHS's request. The proposed collection undermines constitutional rights to speech, association, anonymity, privacy, and due process; violates the Privacy Act; does not comply with the E-Government Act of 2002; and does not meet the requirements of the Paperwork Reduction Act. Moreover, DHS's pursuit of a "generic clearance" for such a controversial proposal impacting constitutional rights, including those of U.S. citizens, is inappropriate.

In April 2021, OMB rejected a proposal that included a similar request to collect social media identifiers on the forms at issue here.<sup>4</sup> At that time, OMB concluded that the proposal did not meet the requirements of the Paperwork Reduction Act (PRA), in part because DHS had not shown the "practical utility" of collecting social media identifiers on these forms.<sup>5</sup> It further instructed that any "similar proposal in the future" needed to demonstrate such utility, which must outweigh the "monetary and social" costs of the collection.<sup>6</sup>

DHS has not done so here. So far, it has provided even less detail about its justifications for this collection than before, including in its published notice only conclusory recitations that collecting social media identifiers is necessary to help verify applicant identities and determine whether they pose a threat. On the other side of the equation, DHS has not addressed the proposal's costs, such as the risks it poses to privacy and to the rights unambiguously guaranteed by the First Amendment, including those of U.S. citizens.

In fact, targeting constitutionally protected speech is a goal the proposed collection apparently seeks to advance. DHS's published notice says it is necessary to comply with Executive Order 14161, which—among other things—establishes a policy of screening

---

<https://www.regulations.gov/document/USCIS-2025-0003-1250> (proposed changes to the I-751 form); and USCIS, USCIS-2025-0003-1241, DHS, September 17, 2025,

<https://www.regulations.gov/document/USCIS-2025-0003-1241> (proposed changes to the I-131 form).

<sup>4</sup> 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](https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202007-1601-001) (hereinafter "OMB Conclusion Re: ICR 202007-1601-001").

<sup>5</sup> OMB Conclusion Re: ICR 202007-1601-001; 44 U.S.C. § 3508 (1995) (Paperwork Reduction Act provision requiring that OMB determine whether a proposed collection of information is necessary and has practical utility before approving it); and 5 C.F.R. § 1320.3(l) (1995) ("Practical utility means 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 (or a person's ability to receive and process that which is disclosed, in the case of a third-party or public disclosure) in a useful and timely fashion.").

<sup>6</sup> OMB Conclusion Re: ICR 202007-1601-001.

people already in the United States for “hostile attitudes” and “hateful ideology,”<sup>7</sup> undefined phrases that have been used to label and punish protected speech.<sup>8</sup> The initial notice was followed by other efforts that demonstrate how DHS plans to use the identifiers it will collect if this proposal is approved. In April of this year, USCIS released statements indicating it would look for “antisemitic activity on social media” and indications of “anti-Americanism” as grounds for denying immigration applications, while providing no concrete guidance as to what those terms encompass, allowing for broad and indiscriminate targeting of protected expression.<sup>9</sup> USCIS updated its policy manual in August to further direct officers to categorize support for “anti-American” and “antisemitic ideologies” as “an overwhelmingly negative factor” in discretionary analyses of immigration benefits applications, which are filed largely by individuals present within the United States.<sup>10</sup> DHS announced it would turn to social media data to make these determinations.<sup>11</sup> The State Department has similarly directed consular

---

<sup>7</sup> Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats, Exec. Order No. 14161, 90 Fed. Reg. 8451 (January 20, 2025), <https://www.federalregister.gov/documents/2025/01/30/2025-02009/protecting-the-united-states-from-foreign-terrorists-and-other-national-security-and-public-safety>.

<sup>8</sup> See, e.g., Darlene Superville, “Trump executive order on Smithsonian targets funding for programs with ‘improper ideology’,” Associated Press, March 27, 2025, <https://apnews.com/article/trump-smithsonian-executive-order-improper-ideology-558ebfab722f603e94e02a1a4b06ed4d>; and Josh Gruenbaum (commissioner, Federal Acquisition Service, General Services Administration) et al., to Dr. Alan M. Garber (president, Harvard University), April 11, 2025, <https://www.harvard.edu/research-funding/wp-content/uploads/sites/16/2025/04/Letter-Sent-to-Harvard-2025-04-11.pdf> (employing undefined phrases of “hateful ideology” to impose ideological admissions, hiring, and programmatic requirements on educational and cultural institutions). See also *Aditya W. H. v. Trump*, No. 25-CV-1976 (KMM/JFD), 2025 WL 1420131, at \*11 (D. Minn. May 14, 2025) (Menendez, J.) (“Executive Order 14161 demonstrates the government’s intent to focus on the vaguely defined category of noncitizens within the United States who purportedly bear ‘hostile attitudes’ toward Americans or U.S. culture and institutions.”).

<sup>9</sup> USCIS, “First 100 Days: USCIS Delivering on Making America Safe Again,” DHS, press release, April 29, 2025, <https://www.uscis.gov/newsroom/news-releases/first-100-days-uscis-delivering-on-making-america-safe-again>; USCIS, “DHS to Begin Screening Aliens’ Social Media Activity for Antisemitism,” DHS, press release, April 9, 2025, <https://www.uscis.gov/newsroom/news-releases/dhs-to-begin-screening-aliens-social-media-activity-for-antisemitism>; and Memorandum from Marco Rubio, Secretary of State, to All Diplomatic and Consular Posts Collective, Re “(U) Action Request: Enhanced Screening and Social Media Vetting for Visa Applicants,” (March 25, 2025), available at <https://bsky.app/profile/marisakabas.bsky.social/post/3llcno2ducc2m>. See also Nasser Eledroos and Rachel Levinson-Waldman, “‘Continuous Vetting’ of All Visa Holders Is Impossible, but the Threat Alone Chills Free Speech,” Brennan Center for Justice, September 25, 2025, <https://www.brennancenter.org/our-work/research-reports/continuous-vetting-all-visa-holders-impossible-threat-alone-chills-free>.

<sup>10</sup> USCIS, “Policy Alert: Clarifying Discretionary Factors in Certain Immigration Benefit Requests,” DHS, August 19, 2025, <https://www.uscis.gov/sites/default/files/document/policy-manual-updates/20250819-DiscretionaryFactors.pdf> [<https://perma.cc/A87H-3HL8>].

<sup>11</sup> USCIS, “USCIS to Consider Anti-Americanism in Immigrant Benefit Requests,” DHS, press release, August 19, 2025, <https://www.uscis.gov/newsroom/news-releases/uscis-to-consider-anti-americanism-in-immigrant-benefit-requests>.

officers to screen visa applicants' online presence for "anti-American" and "antisemitic" activities, and the extensive information-sharing between DHS and the Department of State indicate that the identifiers collected by USCIS could further facilitate that screening.<sup>12</sup>

Combating antisemitism is an important goal. But "antisemitism" is already a broad category with a disputed meaning, and observers across a range of perspectives on the current conflict in the Middle East acknowledge that the administration uses "combating antisemitism" as a fig leaf for targeting constitutionally protected speech supportive of Palestinian rights and/or critical of Israel.<sup>13</sup> It is likely that the proposed collection of identifiers will help facilitate the implementation of these policies and other efforts to target protected speech by identifying speakers online, as well as the broader surveillance and social media monitoring programs undertaken by DHS and other agencies with which DHS shares information.

Moreover, while Executive Order 14161 does direct federal agencies to take a variety of steps to ensure that individuals seeking entry to and already within the United States do not bear hostile attitudes towards American "citizens, culture, government, institutions, or founding principles," and that they are "vetted and screened to the

---

<sup>12</sup> Memorandum from Marco Rubio, Secretary of State to All Diplomatic and Consular Posts Collective, "Enhanced vetting for All Nonimmigrant Visa Applicants Traveling to Harvard University," (May 30, 2025), available at [https://iptp-production.s3.amazonaws.com/media/documents/2025.05.30\\_Dept\\_of\\_State\\_25\\_STATE\\_52014\\_-\\_ACTION\\_REQUEST\\_Enhanced\\_vetting\\_for\\_Qj2s63u.pdf](https://iptp-production.s3.amazonaws.com/media/documents/2025.05.30_Dept_of_State_25_STATE_52014_-_ACTION_REQUEST_Enhanced_vetting_for_Qj2s63u.pdf); and Memorandum from Marco Rubio, Secretary of State to All Diplomatic and Consular Posts Collective, "Expanding Screening and Vetting for FMJ Applicants," (June 18, 2025), available at <https://aboutblaw.com/biDF>. See also Rachel Levinson-Waldman and Naz Balkam, "The Government's Growing Trove of Social Media Data," Brennan Center for Justice, July 21 2025, <https://www.brennancenter.org/our-work/research-reports/governments-growing-trove-social-media-data>.

<sup>13</sup> For example, Kenneth Stern, the lead drafter of the definition of antisemitism used by the administration (which was initially written for the International Holocaust Remembrance Alliance) has said the administration is weaponizing antisemitism to silence political speech. Katy Kline, "Weaponizing antisemitism makes students 'less safe,' says drafter of the definition," NPR, March 20, 2025, <https://www.npr.org/2025/03/20/nx-s1-5326047/kenneth-stern-antisemitism-executive-order-free-speech>. Moreover, conservative and libertarian commentators alike have expressed skepticism at the government's actions against student protesters. See, e.g., Dave Goldiner, "Ann Coulter questions efforts to deport Columbia student Mahmoud Khalil," *New York Daily News*, March 10, 2025, <https://www.nydailynews.com/2025/03/10/ann-coulter-columbia-student-mahmoud-khalil/>; and Robby Soave, "Mahmoud Khalil Is an Easy Call," *Reason*, March 13, 2025, <https://reason.com/2025/03/13/mahmoud-khalil-is-an-easy-call/>. The government itself has acknowledged that student protester Mahmoud Khalil's speech is legal under U.S law, noting that "Under INA section 237(a)(4)(C)(ii), for cases in which *the basis for this determination [of removability] is the alien's past, current, or expected beliefs, statements, or associations that are otherwise lawful*, the Secretary of State must personally determine that the alien's presence or activities would compromise a compelling U.S. foreign policy interest" (emphasis added). Exhibit 1 at 7, *Khalil v. Trump*, 25-cv-1963 (D.N.J. April 12, 2025), ECF 198-1.

maximum degree possible,” it does not require the collection of social media identifiers to accomplish these tasks, nor does it require that any of the vetting and screening occur on social media. As detailed below, there is no evidence that social media screening is useful for vetting people. And it imposes serious costs, regardless of whether or not constitutionally protected speech is intentionally targeted.

With respect to social costs in particular, as our organizations and others have observed on multiple occasions, the collection, retention, and screening of social media information intrudes into privacy, chills free expression and association, and typically is disproportionately deployed against, and disproportionately impacts, minority groups.<sup>14</sup> These risks are enhanced with the proposed extension of this collection to U.S. citizens and residents and the increased monitoring and surveillance that will result, particularly in an environment in which people increasingly rely on social media as a primary channel

---

<sup>14</sup> See, e.g., Brennan Center for Justice, “Brennan Center and Knight Institute Submit Comments Opposing DHS Proposal to Collect Social Media Identifiers,” May 5, 2025, <https://www.brennancenter.org/our-work/research-reports/brennan-center-and-knight-institute-submit-comments-opposing-dhs-proposal>; Brennan Center for Justice, “Brennan Center and EPIC Urge DHS to Withdraw Proposal to Collect Social Media Handles of Visa Applicants,” March 28, 2022, <https://www.brennancenter.org/our-work/research-reports/brennan-center-and-epic-urge-dhs-withdraw-proposal-collect-social-media>; Brennan Center for Justice, “Brennan Center Urges Rejection of Proposal to Collect Social Media Data,” November 5, 2019, <https://www.brennancenter.org/our-work/research-reports/brennan-center-urges-rejection-proposal-collect-social-media-data>; Brennan Center for Justice, “Comments of the Brennan Center Re: DS-160 and DS-156, Application for Nonimmigrant Visa, OMB Control No. 1405-0182; DS-260, Electronic Application for Immigrant Visa and Alien Registration, OMB Control No. 1405-185,” September 27, 2018, [https://www.brennancenter.org/sites/default/files/analysis/OIRA%20Letter\\_9.27.2018.pdf](https://www.brennancenter.org/sites/default/files/analysis/OIRA%20Letter_9.27.2018.pdf); Brennan Center for Justice, “Comments of the Brennan Center re: DS-160 and DS-156, Application for Nonimmigrant Visa, OMB Control No. 1405-0182; DS-260,” May 29, 2018, <https://www.brennancenter.org/sites/default/files/analysis/Comments%20-%20Department%20of%20State%20-%20Visa%20Applicant%20Social%20Media%20Collections%20-%20Public%20Notices%2010260%20-%2010261.pdf>; Electronic Privacy Information Center (hereinafter EPIC), “Comments of the Electronic Privacy Information Center to Department of State,” December 27, 2017, <https://archive.epic.org/EPIC-DOS-Visas-SocialMediaID-Dec2017.pdf>; Center for Democracy & Technology (hereinafter CDT), “Comments of CDT Re: 82 Fed. Reg. 43556, Docket No. DHS-2017-0038,” October 18, 2017, <https://cdt.org/wp-content/uploads/2017/10/Coalition-Letter-Opposing-DHS-Social-Media-Retention-.pdf> (signed by a coalition of civil society organizations); ACLU, “ACLU Comment on Supplemental Questions for Visa Applicants,” October 2, 2017, <https://www.aclu.org/documents/aclu-comment-supplemental-questions-visa-applicants>; Brennan Center for Justice, “Comments of the Brennan Center Re: 82 Fed. Reg. 36180, OMB Control No. 1405-0226; Supplemental Questions for Visa Applicants,” October 2, 2017, <https://www.brennancenter.org/sites/default/files/StateDeptcomments-10.2.2017.pdf>; Brennan Center for Justice, “Coalition Comments re Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 20956,” May 18, 2017, [https://www.brennancenter.org/sites/default/files/State%20Dept%20Information%20Collection%20Comments%20-%202051817\\_3.pdf](https://www.brennancenter.org/sites/default/files/State%20Dept%20Information%20Collection%20Comments%20-%202051817_3.pdf); and Brennan Center for Justice, “Brennan Center Submits Comments on DHS Plan to Collect Social Media Information Through the Visa Waiver Program,” August 22, 2016, <https://www.brennancenter.org/our-work/research-reports/brennan-center-submits-comments-dhs-plan-collect-social-media-information>.

for self-expression and political association.

Because DHS has again failed to demonstrate the practical utility of collecting social media identifiers or to justify any benefits in comparison to the substantial costs articulated herein, its proposal plainly does not meet the requirements of the PRA, as OMB has previously found. We urge OMB to deny this proposal.

### **I. The proposed collection harms core constitutional rights.**

To start, the government has no right to collect and retain the social media handles of U.S. citizens—including pseudonymous and anonymous identifiers—without legal justification. The mandatory collection of all social media identifiers not only invades the privacy of U.S. citizens who have no reason to believe the government is monitoring their social media, but it also undermines their rights to speech, association, and anonymity. The fact that many of the people from whom social media identifiers would be sought are U.S. citizens or permanent residents, or are people who otherwise live in the United States, only makes the following objections more immediate. Indeed, under the proposed collection, DHS will have identifying information sufficient to conduct indefinite surveillance of individuals' social media accounts, even after the adjudication of any benefit has been completed, in the absence of any showing of criminal or other prohibited activity, and using tools ill-suited to the assessment of threats.

We also underscore that non-U.S. citizens in the United States have constitutional rights, given their presence in and connections to the country, as acknowledged in internal government legal analyses<sup>15</sup> and reaffirmed in recent court rulings.<sup>16</sup> They may retain these constitutional rights even when they are outside the country, depending on their legal status and the strength of their U.S. contacts.<sup>17</sup> This proposal thus implicates the constitutional rights of nearly everyone it touches.

---

<sup>15</sup> See Immigrations and Customs Enforcement (hereinafter ICE), DHS, Memorandum re Inadmissibility Based on Endorsing or Espousing Terrorist Activity: First Amendment Concerns, acquired by the Knight First Amendment Institute via FOIA, available at <https://knightcolumbia.org/documents/tgj1l1f1n1j>. See also *Bluman v. Federal Election Commission*, 800 F. Supp. 2d 281, 286 (D.D.C. 2011) (three-judge court) (Kavanaugh, J.) (“We know from more than a century of Supreme Court case law that foreign citizens in the United States enjoy many of the same constitutional rights that U.S. citizens do.”), *aff’d* 565 U.S. 1104 (2012); *United States v. Verdugo-Urquidez*, 494 US 259, 271 (1990) (explaining that aliens “receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country”); and *Bridges v. Wixon*, 326 U.S. 135, 161 (1945) (Murphy, J. concurring) (“But, once 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. None of these provisions acknowledges any distinction between citizens and resident aliens”).

<sup>16</sup> *American Association of University Professors v. Rubio*, No. 25-10685-WGY, 2025 U.S. Dist. LEXIS 193069, at \*6 (D. Mass. Sep. 30, 2025).

<sup>17</sup> ICE, DHS, Memorandum re Inadmissibility, 4–5.

**a. The proposed collection undermines the rights to speech, association, and anonymity.**

Social media platforms are, of course, crucial gathering places for modern public discourse. Billions of people use social media to share news or ideas, connect with others, and spur social or political change. As the U.S. Supreme Court observed nearly a decade ago, websites like Facebook are for many the “principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge.”<sup>18</sup> Consequently, for many people—indeed, for many Americans—the proposed collection will inhibit speech and activity in one of the primary ways they may choose to connect with the world around them. In essence, people affected by the collection—again, including Americans—are faced with a choice they should not have to make: either risk retaliation for their online activity or self-censor.

**i. Impact on Speech**

The proposed collection, if approved, will pressure people to engage in self-censorship by deleting their accounts, disassociating from online connections, limiting their social media postings, or sanitizing their internet presence for fear that their online identifiers may be used to target speech the administration disfavors.<sup>19</sup> These concerns are not hypothetical or conjectural: a recent lawsuit led by the Knight First Amendment Institute documents these impacts in a challenge to the administration’s ideological deportation policy, the umbrella under which cases such as Mahmoud Khalil’s have been initiated, and to which this policy is connected.<sup>20</sup>

Indeed, this administration has openly declared that it is retaliating against people for

---

<sup>18</sup> *Packingham v. North Carolina*, 137 S. Ct. 1730, 1732 (2017).

<sup>19</sup> For example, one study found that fear of government surveillance of the internet had a substantial chilling effect among both U.S. Muslims and broader samples of Internet users. Elizabeth Stoycheff et al., “Privacy and the Panopticon: Online Mass Surveillance’s Deterrence and Chilling Effects,” *New Media & Society* 21, no. 3 (October 2018); and Dawinder S. Sidhu, “The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans,” *University of Maryland Law Journal of Race, Religion, Gender & Class*, 7, no. 2 (September 2007). Even people who said they had nothing to hide were highly likely to self-censor online when they knew the government was watching. See Elizabeth Stoycheff, “Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring,” *Journalism & Mass Communication Quarterly*, 93 no. 2 (June 2016): 307–8.

<sup>20</sup> See *Am. Ass’n of Univ. Professors v. Rubio*, at \*160 (“Secretaries Noem and Rubio . . . acted in concert to misuse the sweeping powers of their respective offices to target non-citizen pro-Palestinians for deportation primarily on account of their First Amendment protected political speech. They did so in order to strike fear into similarly situated non-citizen pro-Palestinian individuals, pro-actively (and effectively) curbing lawful pro-Palestinian speech and intentionally denying such individuals . . . the freedom of speech that is their right.”). See generally *Am. Ass’n of Univ. Professors v. Rubio*, No. 25-cv-10685 (D. Mass. March 25, 2025).

their political speech.<sup>21</sup> These actions have created a climate in which people applying for immigration benefits—with their future in the United States at stake—would be justified in censoring their own online expression in response to being forced to disclose their online identifiers, knowing that the identifiers are likely to be used to further one or more of these official efforts to target constitutionally protected speech.<sup>22</sup>

Even apart from the explicit targeting of speech on topics that are sensitive or that the administration has deemed to be of interest, individuals required to disclose their identifiers could reasonably fear having their social media expression misunderstood or misinterpreted, potentially with dire consequences. Social media communication is often governed by a different set of norms and conventions from in-person communication, making it difficult for outside observers to interpret online speech. Social media posts commonly have context-specific meanings, and can be riddled with abbreviations, memes, sarcasm, slang, jokes, and references to popular culture.<sup>23</sup> And

---

<sup>21</sup> See, e.g., Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats, Exec. Order No. 14161, 90 Fed. Reg. 8451 (executive order, which DHS cites to justify the proposed collection, directing agencies to protect against people with “hostile attitudes” towards American “citizens, culture, government, institutions, or founding principles”); USCIS, “Policy Alert: Clarifying Discretionary Factors” (announcing USCIS will screen social media for “Anti-American activity”); Julia Ainsley, “Inside the DHS task force scouring foreign students’ social media,” NBC News, April 9, 2025, <https://www.nbcnews.com/politics/national-security/dhs-task-force-scouring-foreign-students-social-media-rcna198532> (explaining DHS task force scouring social media of foreign students for evidence of involvement in pro-Palestine and/or anti-Israel protests); Vimal Patel et al., “Nearly 300 Students Have Had Visas Revoked and Could Face Deportation,” *New York Times*, April 7, 2025, <https://www.nytimes.com/2025/04/07/us/student-visas-revoked-trump-administration.html> (same); Memorandum from Marco Rubio, Secretary of State to All Diplomatic and Consular Posts Collective, “Visa Applicants Traveling to Harvard” (May pilot program directing consular officers to review for signs of antisemitism the social media accounts of all applicants seeking a visa to study, teach, or speak at Harvard University); Memorandum from Marco Rubio, Secretary of State to All Diplomatic and Consular Posts Collective, “Vetting for FMJ Applicants” (instructing consular officers to review the online presence of all applicants for student, vocational, and cultural exchange visas to look for support for antisemitic activity, and telling applicants to ensure any private social media accounts are made public); Respondents’ Memorandum of Law in Support of their Motion to Dismiss or to Transfer the Case at 2, *Khalil v. Joyce*, No. 25-cv-1963 (D.N.J. March 12, 2025) ECF 31 (citing expressions of political views as a key—if not sole—basis for barring an individual otherwise here lawfully from staying in the country); First Amendment Petition for Writ of Habeas Corpus and Complaint at 8, *Öztürk v. Trump*, No. 25-cv-10695 (D. Mass. March 28, 2025) (same); and Jack Nicas, “U.S. Threatens to Bar Foreigners Over Remarks About Charlie Kirk,” *New York Times*, September 24, 2025, <https://www.nytimes.com/2025/09/24/world/americas/charlie-kirk-visas-speech.html> (inviting individuals to report social media posts by foreigners that “make light of” the assassination of Charlie Kirk, as a precursor to revoking their visas).

<sup>22</sup> See Rachel Levinson-Waldman and Melanie Geller, “How DHS’s New Social Media Vetting Policies Threaten Free Speech,” Brennan Center for Justice, June 20, 2025, <https://www.brennancenter.org/our-work/analysis-opinion/how-dhss-new-social-media-vetting-policies-threaten-free-speech>.

<sup>23</sup> See Complaint for Declaratory and Injunctive Relief at 23–24, *Doc Society v. Pompeo*, 19-cv-03632 (D.D.C. December 5, 2019), <https://knightcolumbia.org/documents/399e32ad77> (explaining how difficult it

misinterpretations of these posts can have serious consequences.<sup>24</sup> Last year, for example, a sixth grader in Texas was arrested after reportedly saying his “main goal [was] to blow up,” quoting a Tik Tok meme for having success as a musical artist that was mistaken by his teacher for a threat.<sup>25</sup> Elon Musk’s social media posts related to the financial condition and share price of Tesla became the subject of legal proceedings interrogating how seriously they were supposed to be taken, given their lack of clarity to investors who traded in reliance on them.<sup>26</sup>

If DHS moves forward with the proposed collection, it is not clear whether or how it will try to mitigate these glaring risks of misinterpretation. For example, there is no public information about any training officials reviewing social media may receive to stay apprised of how people are communicating online—a difficult task to begin with, given how quickly linguistic conventions evolve on social media platforms.

The use of automated tools only exacerbates these concerns.<sup>27</sup> Rather than enhancing reliability, these tools reflect the biases in their training data, cannot properly account for context, and often perform poorly when they are asked to translate non-English

---

can be to interpret social media posts “without a nuanced understanding of the context in which they are made”).

<sup>24</sup> See, e.g., Bill Chappell, “Supreme Court Tosses Out Man’s Conviction for Making Threat on Facebook,” NPR, June 1, 2015, <http://www.npr.org/sections/thetwo-way/2015/06/01/411213431/supreme-court-tosses-outman-s-conviction-formaking-threats-on-facebook>.

<sup>25</sup> Karina Hollingsworth, “Meme mix-up lands Colorado City Middle School 6th grader in cuffs for terroristic threat,” KTXS 12, August 27, 2024, <https://ktxs.com/news/local/meme-mix-up-lands-colorado-city-middle-school-6th-grader-in-cuffs-for-terroristic-threat>.

<sup>26</sup> Matt McFarland, “‘420 price was not a joke.’ Elon Musk testifies again in trial over controversial tweet,” CNN, January 23, 2023, <https://www.cnn.com/2023/01/23/business/tesla-trial-funding-secured-elon-musk/index.html>. See also Michael German, et al., *Ending Fusion Center Abuses A Roadmap for Robust Federal Oversight*, Brennan Center, December 15, 2022, 3, <https://www.brennancenter.org/our-work/policy-solutions/ending-fusion-center-abuses> (describing DHS and FBI disseminating information that exaggerated the potential for violence at racial justice protests based on posts from far-right accounts that were known to disseminate conspiracy theories); *All Things Considered*, “Police Monitoring of Social Media Sparks Concern in Black and Brown Communities,” NPR, August 21, 2020, <https://www.npr.org/2020/08/21/904646038/police-monitoring-of-social-media-sparks-concerns-in-black-and-brown-communities>; Amy Renee Leiker, “Outcry follows arrest of 2 men over social media post that urged violence in Wichita area,” *Wichita Eagle*, June 8, 2020, <https://www.kansas.com/news/local/crime/article243267626.html>; Ben Conarck, “Sheriff’s Office’s Social Media Tool Regularly Yielded False Alarms,” *Jacksonville*, May 30, 2017, <https://www.jacksonville.com/news/public-safety/metro/2017-05-30/sheriff-s-office-s-social-media-tool-%20regularly-yielded-false>; and J. David Goodman, “Travelers Say They Were Denied Entry to U.S. for Twitter Jokes,” *New York Times*, January 30, 2012, <https://thelede.blogs.nytimes.com/2012/01/30/travelers-say-they-were-denied-entry-to-u-s-for-twitter-jokes>.

<sup>27</sup> Alfred Ng, “The worries about AI in Trump’s social media surveillance,” *Politico*, April 8, 2025, <https://www.politico.com/newsletters/digital-future-daily/2025/04/08/the-worries-about-ai-in-trumps-social-media-surveillance-00279255>; and Ainsley, “Inside the DHS task force.”

languages.<sup>28</sup> For instance, the administration’s recent efforts to automatically flag content as part of its efforts to purge programs and references related to “DEI” [Diversity, Equity, and Inclusion] from the federal government have produced a number of glaring errors. The government mistakenly put on leave a federal employee who managed relationships with businesses held by private equity, because of the inclusion of the term “equity.”<sup>29</sup> It initially eliminated references to “inequity” and “inclusion” from an IRS employee handbook, even though these references were to the “inequity” of holding on to taxpayer money and the “inclusion” of a taxpayer identification number on a form.<sup>30</sup> And it flagged posts about the World War II bomber Enola Gay for deletion from the Defense Department’s databases and website because of the use of the word “gay.”<sup>31</sup>

Commercial tools from the largest companies in the world have failed dismally as well. As recently as 2023, Meta’s auto-translation feature on Instagram added “Palestinian terrorist” to the profile bios of some users solely because the bios featured a Palestinian flag and an Arabic phrase of prayer and gratitude.<sup>32</sup> Even contemporary large language model tools that claim high levels of accuracy in interpreting and classifying text generate frequent and blatant false positives. In one notable example, a tool identified parts of the U.S. Constitution and Bible as AI-generated.<sup>33</sup>

---

<sup>28</sup> Eledroos and Levinson-Waldman, “‘Continuous Vetting’ of All Visa Holders Is Impossible”; and CDT, “Automated Tools for Social Media Monitoring Irrevocably Chill Millions of Noncitizens’ Expression,” April 15, 2025, <https://cdt.org/insights/automated-tools-for-social-media-monitoring-irrevocably-chill-millions-of-noncitizens-expression/>. For more discussion on this issue, which we explained in our 2019 comment to DHS in response to its previous and identical proposal to collect social media identifiers from those applying for immigration-related benefits, see Brennan Center for Justice, “Brennan Center Urges Rejection of Proposal to Collect Social Media Data,” November 5, 2019, 7–8, <https://www.brennancenter.org/our-work/research-reports/brennan-center-urges-rejection-proposal-collect-social-media-data>.

<sup>29</sup> Katherine Tangalakis-Lippert and Jack Newsham, “DOGE’s anti-DEI drive flagged these programs. Only they weren’t DEI,” *Business Insider*, March 11, 2025, <https://www.businessinsider.com/doge-wrongly-flagged-jobs-programs-dei-equity-2025-3>.

<sup>30</sup> Rachel Leingang, “Trump’s demands to drop DEI leads to deletion of unrelated federal pages,” *Guardian*, January 31, 2025, <https://www.theguardian.com/us-news/2025/jan/31/trump-administration-dei-irs>.

<sup>31</sup> Tara Copp, Lolita C. Baldor, and Kevin Vineys, “War heroes and military firsts are among 26,000 images flagged for removal in Pentagon’s DEI purge,” Associated Press, March 7, 2025, <https://apnews.com/article/dei-purge-images-pentagon-diversity-women-black-8efcfaec909954f4a24bad0d49c78074>.

<sup>32</sup> Josh Taylor, “Instagram apologises for adding ‘terrorist’ to some Palestinian user profiles,” *Guardian*, October 19, 2023, <https://www.theguardian.com/technology/2023/oct/20/instagram-palestinian-user-profile-bios-terrorist-added-translation-meta-apology>.

<sup>33</sup> Benj Edwards, “Why AI writing detectors don’t work,” *Arstechnica*, July 14, 2023, <https://arstechnica.com/information-technology/2023/07/why-ai-detectors-think-the-us-constitution-was-written-by-ai/>.

Notwithstanding these known shortfalls, a January 2025 Inspector General report evaluating DHS’s oversight of its use of artificial intelligence found that it “did not have adequate governance processes to monitor AI compliance with privacy and civil rights and civil liberties requirements.”<sup>34</sup> The use of this technology will thus only exacerbate, not mitigate, individuals’ reasonable concerns about the stakes of having their social media data incorporated into determinations related to permanent residency or citizenship.

*ii. Impact on Association*

The proposed collection would open the door to ongoing online surveillance of the associational activities of U.S. persons, including citizens, legal permanent residents, and others physically present in the country. Whomever the proposal overtly targets, social media is inherently interactive. A person’s social media profile doesn’t just depict their own activity; it reveals who has shared, liked, commented on, or responded to their activity. The proposed collection threatens to chill these associational activities in multiple ways.

First, in addition to the social media identifiers of the applicants themselves, DHS also explicitly seeks from applicants the social media identifiers of relatives whose relationship may be relevant to the benefit sought. For example, on the I-751 (“Petition to Remove Conditions on Residence”), DHS would explicitly require applicants to disclose the social media handles of their U.S. citizen relatives, though it fails to make this point clear in its regulatory notice.<sup>35</sup> The proposed collection’s broad definition of social media also requires applicants to disclose their business and organizational accounts—explained as “university alumni, hobby group or club, etc.” accounts—which further risks revealing applicants’ networks and associations.<sup>36</sup> Consequently, DHS will end up reviewing the speech and associations of a wide range of an applicant’s contacts, from friends and family members to business associates and acquaintances. The proposed collection thus imposes a significant burden on their freedom of association.

Second, applicants are at risk of being held accountable for the speech or actions of people with whom they have interacted. In one notable case, DHS officials barred a Lebanese student of Palestinian descent from entering the country to begin his studies at Harvard based on the content of his friends’ social media posts. The posts simply expressed political views that contrasted with positions of the U.S. government, and the

---

<sup>34</sup> 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, 3, <https://www.oig.dhs.gov/sites/default/files/assets/2025-02/OIG-25-10-Jan25.pdf>.

<sup>35</sup> USCIS, USCIS-2025-0003-1242.

<sup>36</sup> USCIS, USCIS-2025-0003-1242. See also USCIS, USCIS-2025-0003-1230, DHS, September 17, 2025, <https://www.regulations.gov/document/USCIS-2025-0003-1230> (the proposed I-131 form).

student had neither written nor engaged with them.<sup>37</sup>

Finally, friends and relatives of the applicant may self-censor as well, to avoid jeopardizing the applicant's chances of receiving a green card, preserving legal status in the United States, getting asylum, or obtaining other immigration benefits. These impacts will not be ephemeral, given that adjudication times can be long: the wait time for a petition to remove conditions on an applicant's permanent residence, for instance, is estimated to be approximately two years.<sup>38</sup>

### *iii. Impact on Anonymous Speech and Private Association*

The proposed collection does not exempt identifiers used to engage in pseudonymous or anonymous speech; rather, it broadly seeks any identifying information that could be associated with a person's online presence.<sup>39</sup> By compelling applicants to disclose any identifiers they have used on social media platforms during the preceding five years—including pseudonymous identifiers—the proposed collection unquestionably burdens applicants' rights to communicate anonymously and associate privately online, rights that are protected by the First Amendment.<sup>40</sup> “[A]n author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First

---

<sup>37</sup> Karen 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>.

<sup>38</sup> USCIS, “Historical National Median Processing Time (in Months) for All USCIS Offices for Select Forms By Fiscal Year,” DHS, accessed October 16, 2025, <https://egov.uscis.gov/processing-times/historical>.

<sup>39</sup> See Collection Notice. Going beyond past proposals, the proposed instructions that accompany the relevant forms say: “If the social media platform does not use a handle, provide the relevant associated identifiable information used to access the platform (for example, email, phone number).” The instructions to applicants now offer a broad definition of “social media” that includes certain more privacy-focused applications that do not require users to create a handle—such as Telegram or WhatsApp. Even if applicants are otherwise already required to provide their emails and phone numbers, by explicitly asking for this information, DHS would have a more comprehensive view, at a minimum, of the digital channels they use to communicate; this information will also make it easier to identify previously unknown participants in, for instance, a WhatsApp chat. In any event, the broad framing in this aspect of the proposed collection suggests a focus beyond identifiers that publicly identify a person and an intention to sweep in activity an applicant wants to keep private.

<sup>40</sup> See, e.g., *Watchtower Bible & Tract Soc’y of New York, Inc. v. Vill. of Stratton*, 536 U.S. 150, 153, 166 (2002); *Buckley v. Am. Constitutional Law Found., Inc.*, 525 U.S. 182, 200 (1999); *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995) (Stevens, J.) (“Anonymity is a shield from the tyranny of the majority... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.”); *Talley v. California*, 362 U.S. 60 (1960); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958); *Sweezy v. New Hampshire*, 354 U.S. 234 (1957); Electronic Frontier Foundation, “Anonymity,” accessed October 16, 2025, <https://www EFF.org/issues/anonymity>.

Amendment.”<sup>41</sup> And “compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [other] forms of governmental action.”<sup>42</sup>

On many social media platforms, it is common for users to create anonymous accounts not associated with their identities. People may create such accounts for a variety of reasons, as extensively documented in an amicus brief filed by Twitter (now X), Reddit, and the Internet Association (a lobbying group for internet companies) in support of the Brennan Center and the Knight First Amendment Institute’s lawsuit challenging the State Department’s collection of social media identifiers on its visa application forms.<sup>43</sup>

Many people use pseudonymous social media identifiers to speak about sensitive or controversial issues, and to shield themselves, their families, or their associates from reprisals by state or private actors. For example, political activists facing retribution or harm may use pseudonymous social media identifiers to protect themselves from having their identity linked to their online speech. Users from countries where it is physically dangerous to identify as lesbian, gay, bisexual, or transgender (LGBT) might create a pseudonymous or anonymous account to protect their identity while interacting with the LGBT community online. And a person may create a pseudonymous handle to discuss sensitive topics, such as fertility issues they are experiencing, with online communities intended to provide support for people going through the same challenges. This collection will put them in the untenable position of choosing between knowing that federal officials could be aware of their most personal matters and speaking candidly in venues where they are able to get help.

In sum, the proposed collection would directly injure applicants’ First Amendment interests in maintaining their anonymity and protecting the privacy of their online associations. Moreover, as noted above, it may put people who use pseudonymous identifiers in danger. Without a scintilla of evidence that the proposed collection will materially contribute to the vetting and screening process, people should not be required to expose themselves to the risk that comes with unclocking their—and others’—online identities.

**b. The proposed collection undermines individual privacy.**

A person’s social media presence—especially across platforms and over time—can

---

<sup>41</sup> McIntyre, 514 U.S. at 342.

<sup>42</sup> NAACP, 357 U.S. at 462.

<sup>43</sup> *Amicus Curiae* Brief of Twitter, Inc., Reddit, Inc., and Internet Association in Support of Plaintiffs’ Opposition to Defendants’ Motion to Dismiss at 11–14, *Doc Society* (D.D.C. May 28, 2020), <https://knightcolumbia.org/documents/4b2d5c21ad>.

reveal much about them. Indeed, DHS itself has categorized social media handles as “Sensitive PII” whose disclosure could “result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.”<sup>44</sup> This information is far more capacious, detailed, and sensitive than what is required to adjudicate an immigration application.

As the Electronic Frontier Foundation (EFF) has explained, social media data is akin to cell phone and location information, data to which the Supreme Court has afforded constitutional protections in light of the fact that it “collects in one place many distinct types of information ... that reveal much more in combination than any isolated record.”<sup>45</sup> Reams of “posts, photos and videos, and [disclosures of] group membership” can illuminate ethnicity, political views, religious practices, gender identity, sexual orientation, personality traits, and embarrassing—but legal—practices.<sup>46</sup> Even if DHS officials do not intentionally look for this information, the fact that they have it easily accessible increases the risk of bias in the adjudication of a given application as well as the risk that it will be misappropriated for purposes beyond the screening for immigration benefits envisioned in the original collection, as further discussed below.

The proposed collection of social media identifiers—including those of U.S. citizens—enables the continuous monitoring of individuals’ online presence, revealing intimate details of their private lives.<sup>47</sup> People are left to manage privacy settings across a range of platforms that frequently change with little more than boilerplate notice. Making sure that these settings properly capture user intent can be difficult, leading people to inadvertently disclose information meant to be private. In one notable example, researchers were able to accurately pinpoint where Twitter (now X) users lived, worked,

---

<sup>44</sup> See, e.g., Privacy Office, Privacy Threshold Analysis Version Number: 04-26, DHS, March 14, 2017, 8, <https://www.brennancenter.org/sites/default/files/2022-03/PTA%202017%20SM%20as%20SPII.pdf> (noting that social media handles constitute “stand-alone Sensitive Personally Identifiable Information”); and Privacy Office, Privacy Threshold Analysis Version Number: 01-2014, DHS, January 2014, 4n2, <https://www.brennancenter.org/sites/default/files/2022-02/PTA%20for%20OI%20and%20OPR.pdf>.

<sup>45</sup> Sophia Cope and Saira Hussain, “EFF to Court: Social Media Users Have Privacy and Free Speech Interests in Their Public Information,” Electronic Frontier Foundation, June 30, 2020, <https://www.eff.org/deeplinks/2020/06/eff-court-social-media-users-have-privacy-and-free-speech-interests-their-public>.

<sup>46</sup> Brief of *Amicus Curiae* Electronic Frontier Foundation at 10, *Doc Society* (D.D.C. May 29, 2020) (quoting *United States v. Jones*, 565 U.S. 400 (2012) (Sotomayor, J., concurring)).

<sup>47</sup> In particular, as contemporary debates about political strategy have illuminated, political discourse increasingly happens on social media. Whether or not a person posts a lot about politics, people increasingly telegraph their preferences on social media by engaging with offerings that are digitally distributed, all of which foster discrete online communities to generate engagement and inform programming. And when people consume and engage with legacy media (e.g., Fox, MSNBC, or CNN), they may do it through social media itself. Political dispositions that would previously have been evident from speaking with someone or knowing what channels they like to have on in the background in their living room may now be more easily discerned from a scan of their social media accounts.

prayed, or spent time out at night based on geolocation data embedded in their tweets, even though many did not realize they had enabled the location-sharing setting in the first place.<sup>48</sup>

The proposed collection's broad definition of social media to include text messaging platforms like WhatsApp, Telegram, and GroupMe exacerbates these privacy intrusions. Unlike individuals on public platforms like Facebook and Twitter, users of these messaging services do not expect that their engagement on these tools will be made public. Indeed, WhatsApp and Telegram market themselves as privacy-focused messaging services that can provide customers with enhanced privacy settings.<sup>49</sup>

Recent State Department directives requiring student and exchange program visa applicants to set their profiles to public further illustrates the privacy threats at stake. The department's guidance explains that an applicant's failure to make accounts public "reflects evasiveness or otherwise calls into question the applicant's credibility."<sup>50</sup> However, there are multiple legitimate reasons people choose to keep their accounts private, including women and LGBTQ+ individuals seeking safety from online harassment and physical violence,<sup>51</sup> activists and journalists seeking protection from political persecution, and individuals simply seeking to keep their personal lives away from the public eye. The recent requirement directing publication of private social media accounts suggests applicants for immigration benefits may be exposed to additional privacy risks in the future.

---

<sup>48</sup> Kostas Drakonakis et al., "Please Forget Where I was Last Summer: The Privacy Risk of Location (Meta)Data," *The Network and Distributed System Security Symposium* (2019), <https://arxiv.org/pdf/1901.00897.pdf>. See also Joseph Cox, "Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics," *404 Media*, October 23, 2024, <https://www.404media.co/inside-the-u-s-government-bought-tool-that-can-track-phones-at-abortion-clinics/> (explaining how location data and inferences drawn from other posts could reveal a visit to a family planning clinic, risking criminal punishment as abortion becomes functionally illegal in some states).

<sup>49</sup> See, e.g., WhatsApp, "Introducing Advanced Chat Privacy: Enhanced Protection for Your Most Sensitive Conversations," April 23, 2025, <https://blog.whatsapp.com/introducing-advanced-chat-privacy?lang=en>.

<sup>50</sup> Memorandum from Marco Rubio, Secretary of State to All Diplomatic and Consular Posts Collective, "Vetting for FMJ Applicants."

<sup>51</sup> See National Domestic Violence Hotline, "Internet Safety," accessed October 16, 2025, <https://www.thehotline.org/plan-for-safety/internet-safety/> (encouraging domestic violence survivors to maintain strict privacy settings and a limited online presence); and Human Rights Campaign Foundation, *Online Harassment, Offline Violence: Unchecked Harassment of Gender-Affirming Care Providers and Children's Hospitals on Social Media, And Its Offline Violent Consequences*, December 13, 2022, <https://www.hrc.org/press-releases/new-human-rights-campaign-foundation-report-online-hate-real-world-violence-are-inextricably-linked>.

**c. It is difficult for people to comply with the proposed collection, in contravention of their due process rights.**

In addition to the risks connected with the collection, disclosure, and sharing of this information, simply complying with the proposed collection will not be straightforward for applicants, given the lack of clear notice about its precise requirements and the fact that compliance is contingent on the cooperation of third parties.

While its initial notice failed to provide clear guidance to applicants,<sup>52</sup> USCIS's revised notice raises new issues. Going well beyond past proposals, the revised instructional materials accompanying the relevant forms now define "social media" broadly to include "websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact" including "blogs," "broadcast/push text messaging services," and "other emerging technologies." The instructions provide non-exhaustive lists of examples such as Facebook, X, and Instagram, as well as messaging services that wouldn't typically be considered "social media," like WhatsApp, Telegram, and GroupMe.<sup>53</sup>

The instructions also include ambiguous language about disclosing organizational accounts, directing applicants to indicate whether each disclosed social media account is "a personal, business, or organization (for example, university alumni, hobby group or club, etc.) account." This sweeping and vague language not only exacerbates the proposed collection's chilling effect and privacy invasions, but also fails to provide clear guidance to applicants, making it likely that applicants will be denied for inadvertent failure to provide a long-forgotten identifier or confusion over what is supposed to be disclosed. It will also make it easier for the government to find pretextual reasons to reject disfavored applicants.

In asking applicants to compile the identifiers of relatives, the proposed collection also makes them responsible for the actions of a third party. The applicant is asked to solicit this sensitive information from people with whom they may not have a good relationship, who may be less scrupulous about the comprehensiveness of their disclosures, who may have an incentive to withhold information they don't want the applicant to know, or who may simply not remember all the relevant information.

---

<sup>52</sup> None of the instructional materials accompanying the relevant forms defined "social media," only giving non-exhaustive lists of examples such as "Facebook, X, Instagram, etc." See, e.g., USCIS, USCIS-2025-0003-0031, DHS, March 5, 2025, 4, <https://www.regulations.gov/document/USCIS-2025-0003-0031> (initial proposed I-751 form instructions); USCIS, USCIS-2025-0003-0035, DHS, March 5, 2025, 4, 2025, <https://www.regulations.gov/document/USCIS-2025-0003-0035> (initial proposed I-829 form instructions); and USCIS, USCIS-2025-0003-0015, DHS, March 5, 2025, 6, <https://www.regulations.gov/document/USCIS-2025-0003-0015> (initial proposed I-485 form instructions).

<sup>53</sup> See, e.g., USCIS, USCIS-2025-0003-1250.

Particularly alarming, DHS proposes to collect and retain the social media identifiers of applicants' minor children, without any mention of protocols governing the review, privacy, and security of such information.<sup>54</sup> In addition, the challenges associated with interpreting social media properly are particularly salient when it comes to reviewing the online activity of younger people, who are especially disposed to use shorthand or other communicative conventions that are unlikely to be intelligible to a government official, and to be hastier or less moderated in their online communications. Recognizing the particular risks that social media monitoring by law enforcement poses to young people, organizations such as the American Academy of Pediatrics have released public materials for families on how to protect their children who use social media from these risks.<sup>55</sup> We have also documented these issues in the context of social media surveillance in U.S. schools.<sup>56</sup>

Ultimately, we are concerned that a failure to comply with the proposed collection, even inadvertently, may be used as a reason to deny people immigration benefits or strip them of status down the road. Much is at stake for applicants, from failing to qualify as a refugee or asylee when fleeing a war zone to being denied U.S. citizenship or permanent residency. For these reasons, at a bare minimum, DHS must clarify in far greater detail what is necessary to comply with the requirements of this proposed collection.

## **II. DHS's retention and sharing of social media identifiers violates the Privacy Act and amplifies these harms to individuals' rights.**

DHS will store the identifiers it collects in databases with long retention periods and may share them within and outside the federal government for a range of broadly defined purposes, in contravention of the requirements of the Privacy Act.<sup>57</sup> Further, this

---

<sup>54</sup> See, e.g., USCIS, USCIS-2025-0003-1250 (proposed changes to the I-751 form, which ask for the social media identifiers of the applicant's children).

<sup>55</sup> American Academy of Pediatrics, "Law Enforcement, Social Media, and Youth: Family Tips," January 21, 2025, <https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/qa-portal/qa-portal-library/qa-portal-library-questions/law-enforcement-social-media-and-youth-family-tips>.

<sup>56</sup> Brennan Center for Justice, "Schools: Social Media Surveillance," accessed October 16, 2025, <https://www.brennancenter.org/issues/protect-liberty-security/social-media/schools-social-media-surveillance>.

<sup>57</sup> Privacy Act: Privacy Act of 1974, System of Records, DHS-2017-0038, 82 Fed. Reg. 43556 (September 18, 2017), <https://www.federalregister.gov/d/2017-19365> (hereinafter "DHS-2017-0038 SORN") (e.g., Routine Use H: "To 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."). Indeed, DHS policy—including a recent executive order on "eliminating information silos"—explicitly encourages this type of data dissemination.

retention and dissemination of social media handles will amplify the chilling effects and constitutional impacts of the proposed collection, as applicants and their affected relatives may reasonably believe they are being monitored at any time—and for purposes wholly untethered from immigration benefit adjudication—after they disclose their identifiers. Simply put, the proposed collection will give DHS the ability to indefinitely monitor and share the social media identifiers of millions of people in the United States, with functionally no oversight to mitigate the concomitant data privacy and civil liberties risks.<sup>58</sup>

**a. The proposed collection violates the Privacy Act.**

The Privacy Act, passed in the wake of Watergate, sought to restore trust in the government by establishing limits on the information the government collects about the public.<sup>59</sup> The statute, which incorporates key principles known as the Fair Information Practice Principles, requires that agencies maintain only information that is “relevant and necessary” to a lawful agency purpose; ensure that all records are accurate, timely, and complete; and establish safeguards to protect the security and confidentiality of records.<sup>60</sup> It also gives the public the ability to determine what records pertaining to them are collected, maintained, used, or disseminated by an agency, with certain exceptions.

The social media identifier collection proposal is in direct conflict with the requirements of the Privacy Act. It does not specify why social media handles are needed, who will access this information, how it will be used or stored, what information is relevant to consideration of an application, or when collected information will be disclosed. The notice says only that social media handles will be “collected from certain populations of individuals” and that the collection “is necessary for the enhanced identity

---

Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, Exec. Order No. 14243, 90 Fed. Reg. 13681

(March 20, 2025), <https://www.federalregister.gov/documents/2025/03/25/2025-05214/stopping-waste-fraud-and-abuse-by-eliminating-information-silos>.

<sup>58</sup> See Levinson-Waldman and Balkam, “The Government’s Growing Trove of Social Media Data.” For example, in recent years, about 800,000 people annually have become naturalized citizens. Under the proposed collection, each one of them would have had to provide, sometimes on multiple occasions, their social media identifiers to DHS. USCIS, “Naturalization Statistics,” DHS, January 24, 2025, <https://www.uscis.gov/citizenship-resource-center/naturalization-statistics>.

<sup>59</sup> *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579), Source Book on Privacy: Joint Committee Print from S. Comm. on Gov’t Operations, H. Comm. on Gov’t Operations, and H. Subcomm. on Gov’t Information and Individual Rights*, 94 Cong., 2d, 4 (1976), [https://www.justice.gov/d9/privacy\\_source\\_book.pdf](https://www.justice.gov/d9/privacy_source_book.pdf). For a more detailed discussion of the rationale for the Privacy Act, see the introduction in Office of Privacy and Civil Liberties, “Overview of the Privacy Act: 2020 Edition,” Department of Justice, updated October 4, 2022, <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction>.

<sup>60</sup> 5 U.S.C. §§ 522a(e)(1), (5), (10) (2025).

verification, vetting and national security screening, and inspection conducted by USCIS” in order to “help validate an applicant’s identity and determine whether such grant of a benefit poses a security or public-safety threat to the United States.”<sup>61</sup> This vague language is inadequate to satisfy the requirements of the Privacy Act.

The requirement that applicants provide the social media identifiers of certain family members creates additional conflicts with the law. The Privacy Act requires that information must be collected wherever possible directly from the person to whom it relates “when the information may result in adverse determinations about an individual’s rights, benefits, and privileges under Federal programs.”<sup>62</sup> Because the notice and its accompanying documentation provide little information about precisely how this information will be used, it is not known whether these handles—and the other sensitive information they reveal—may ultimately be used to deny immigration benefits to family members who are not themselves U.S. citizens, or even to deny other types of federal benefits to citizens and lawful permanent residents.

The data collection instruments and accompanying instructions also provide little additional information. For example, the Privacy Notice on the instructions for the revised Form I-751 says only that the information will be used to “grant or deny the immigration benefit you are seeking.”<sup>63</sup> That minimal information does not satisfy the requirements of the Privacy Act because it does not make clear, for example, whether DHS will maintain only the information that is “relevant and necessary” to the purposes set out in the notice and the executive order, ensure the “accuracy, relevance, timeliness, and completeness” of the information, or “establish safeguards” for protecting the information.<sup>64</sup>

The proposed collection of social media identifiers will also likely violate the Privacy Act’s bar on maintaining records of U.S. persons’ First Amendment-protected activity.<sup>65</sup> To start, social media handles themselves may reflect First Amendment-protected activity, such as Reddit handles reflecting political speech (e.g., “u/BidenSucks” or “u/TrumpIsAwful”) or accounts affiliated with an organization like a social media book club. The collection of social media identifiers also facilitates increased monitoring and collection of people’s social media data, which reveals online expression, religious and political beliefs, networks, and associations. As we highlight throughout this comment, information about the First Amendment-protected activities of citizens and legal

---

<sup>61</sup> See Collection Notice.

<sup>62</sup> 5 U.S.C. § 522a(e)(2) (2025).

<sup>63</sup> USCIS, USCIS-2025-0003-1240, DHS, September 17, 2025, 11, <https://www.regulations.gov/document/USCIS-2025-0003-1240> (the proposed I-751 form instructions).

<sup>64</sup> 5 U.S.C. §§ 522a(e)(1), (5), (10) (2025).

<sup>65</sup> 5 U.S.C. § 522a(e)(7) (2025).

permanent residents will almost certainly be incorporated into applicants' files. DHS's statutory authority to determine eligibility for immigration benefits does not permit this wholesale collection and maintenance of social media data relating to political beliefs, association, and religion.

The exceptions to the Privacy Act's provisions that would permit the collection of records describing how individuals exercise their First Amendment rights likely do not apply here. Agencies may only maintain these records when "expressly authorized by statute, or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."<sup>66</sup> But the proposed collection is not "expressly authorized" by any statute, including the Homeland Security Act.<sup>67</sup> And the law enforcement exception likely would not apply to the administrative review of applicants seeking immigration-related benefits.<sup>68</sup>

The Privacy Act also requires agencies to publish a system of records notice (SORN) to instruct the public about the "existence and character" of a database when it is revised or a new one is rolled out, if the database is not covered by an existing SORN.<sup>69</sup> The social media handle proposal indicates that it will use the social media records in accordance with existing SORNs, but existing SORNs do not adequately explain how social media handles will be collected, stored, or disclosed. For example, the I-751 instruction sheet's Privacy Notice indicates that it will follow approved routine uses for the DHS/USCIS-007 Benefits Information System, but that system allows only for storage of publicly available social media information, not individual social media handles.<sup>70</sup>

Similarly, although two forms included in the notice—the I-751 and I-829—envision collection of the social media identifiers of an applicant's family members, existing DHS SORNs referenced in the instructions accompanying these proposed new forms do not clearly allow for maintenance of social media identifiers of applicants' family

---

<sup>66</sup> 5 U.S.C. § 552a(e)(7) (2025).

<sup>67</sup> See, e.g., *Stoianoff v. Comm'r of Dep't of Motor Vehicles*, 12 F. App'x 33, 35 (2d Cir. 2001) (finding express statutory authority in the Social Security Act for a parallel Privacy Act claim); *Clarkson v. I.R.S.*, 678 F.2d 1368, 1374 (11th Cir. 1982).

<sup>68</sup> See, e.g., *Clarkson*, 678 F.2d at 1374 (quoting *Jabara v. Kelley*, 476 F. Supp. 561, 581 (E.D. Mich.1979)) ("Merely because (an agency) may act within its authority by monitoring the public or private speeches of a person in the course of a legitimate security investigation does not give it the right to maintain records relating to the contents of these speeches where the investigation does not focus on a past or anticipated specific criminal act.").

<sup>69</sup> 5 U.S.C. § 522a(e)(4) (2025).

<sup>70</sup> Compare USCIS, USCIS-2025-0003-1240, 11; with Privacy Act: Privacy Act of 1974, System of Records, DHS-2019-0042, 84 Fed. Reg. 54622 (October 10, 2019), <https://www.federalregister.gov/documents/2019/10/10/2019-22156/privacy-act-of-1974-system-of-records>.

members.<sup>71</sup> The Alien Files (A-Files) SORN only allows for maintenance of records for “relatives and associates of any of the individuals listed” who are “subject to” the Immigration and Nationality Act. Many family members will be outside that scope.<sup>72</sup> The Immigration Biometric and Background Check SORN does not explicitly provide for maintenance of social media handles at all.<sup>73</sup>

**b. Retention of identifiers will enable ongoing surveillance of U.S. persons.**

DHS maintains an official record of an individual’s visa and immigration history in their A-File, which is stored for 100 years after the individual’s date of birth.<sup>74</sup> A-Files contain information including “social media handles, aliases, associated identifiable information, and search results”—meaning this revealing data will be retained even once the individual becomes a naturalized citizen. This is the case even though the government could not otherwise compel citizens to disclose their social media identifiers.

In addition, DHS policy allows the dissemination of A-File information not only to other DHS components with a “need to know” the information—a broad permission, given DHS’s sprawling mandate—but also to “appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies.” It even permits sharing of data contained within a person’s A-File with current and prospective employers, among other third parties.<sup>75</sup> As a result, this sensitive data, to which the government would not otherwise have access, may be shared freely with a host of entities, with scant information about the purposes to which it may be put.

By enabling the long-term retention of social media data, the proposed collection

---

<sup>71</sup> See USCIS, USCIS-2025-0003-1250; USCIS, USCIS-2025-0003-1256, DHS, September 17, 2025, <https://www.regulations.gov/document/USCIS-2025-0003-1256> (the proposed I-829 form instructions); DHS-2017-0038 SORN; Privacy Act: Privacy Act of 1974, System of Records, DHS-2018-0003, 83 Fed. Reg. 36950 (July 31, 2018), <https://www.federalregister.gov/documents/2018/07/31/2018-16138/privacy-act-of-1974-system-of-records>; and Privacy Act: Privacy Act of 1974, System of Records, DHS-2018-0002, 83 Fed. Reg. 36792 (July 31, 2018), <https://www.federalregister.gov/documents/2018/07/31/2018-16137/privacy-act-of-1974-implementation-of-exemptions-department-of-homeland-security-us-citizenship-and>.

<sup>72</sup> DHS-2017-0038 SORN at 43559.

<sup>73</sup> DHS-2018-0003.

<sup>74</sup> DHS-2017-0038 SORN at 43561.

<sup>75</sup> DHS-2017-0038 SORN at 43557. In addition, this administration has been known to repurpose data initially collected to facilitate other government functions (e.g., collecting taxes or resettling unaccompanied children who crossed the border with families in the United States) for more punitive law enforcement purposes. See, e.g., Wilfredo A. Ferrer et al., “IRS and ICE Memorandum of Understanding Will Drive Tax Payroll Audits and Investigations,” Holland & Knight, April 21, 2025, <https://www.hklaw.com/en/insights/publications/2025/04/irs-and-ice-memorandum-of-understanding-will-drive-tax>; and Jesus Rodriguez, “Ending the Misuse of Immigrants’ Data,” Brennan Center for Justice, May 20, 2021, <https://www.brennancenter.org/our-work/analysis-opinion/ending-misuse-immigrants-data>.

essentially creates a mechanism for the federal government to monitor the speech and associations of U.S. citizens, when doing so would typically be governed by laws and regulations on the collection and dissemination of domestic intelligence activities. DHS's Office of Intelligence & Analysis, for example, is required to have a "reasonable belief" that collected information serves a national or departmental mission, such as countering terrorism; more recently, it implemented a requirement to document justifications for initiating surveillance.<sup>76</sup> Even as we have criticized these rules for being overly permissive, they still at least lay out *some* boundaries and incorporate a modicum of process for the kind of surveillance that this proposed collection would enable DHS to do.<sup>77</sup> By contrast, it is not at all clear what limitations USCIS intends to apply in the first instance, if any.

**c. DHS fails to assess the privacy risks of the proposed collection.**

Despite the breadth of the current proposal, including the collection of new information, DHS has not conducted a privacy impact assessment (PIA) that complies with the E-Government Act of 2002, which requires federal agencies to conduct PIAs when initiating a new collection of information and to ensure that personal information has sufficient privacy protections.<sup>78</sup> Nor has DHS identified an existing PIA that covers the collection of such information.

As one example, the instructions for Form I-751 indicate that DHS will follow the routine uses in the PIA for the Computer Linked Application Information Management System and Associated Systems, or CLAIMS.<sup>79</sup> But the CLAIMS PIA does not even reference collection of social media handles for family members, let alone provide sufficient detail to infer how their social media handles and those of applicants will be evaluated when considering eligibility for an immigration benefit.<sup>80</sup>

Simply put, DHS seeks to make a major change: to begin collecting social media handles of applicants for immigration benefits and of their family members. And it does

---

<sup>76</sup> Office of Intelligence and Analysis, *Policy Manual 2025*, DHS, January 16, 2025, 30–34, [https://www.dhs.gov/sites/default/files/2025-03/25\\_0313\\_ia\\_office-of-intelligence-and-analysis\\_policy-manual.pdf](https://www.dhs.gov/sites/default/files/2025-03/25_0313_ia_office-of-intelligence-and-analysis_policy-manual.pdf).

<sup>77</sup> Spencer Reynolds, "How DHS Laid the Groundwork for More Intelligence Abuse," Brennan Center for Justice, March 5, 2025, <https://www.brennancenter.org/our-work/analysis-opinion/how-dhs-laid-groundwork-more-intelligence-abuse-0>; and Spencer Reynolds and Faiza Patel, *A New Vision for Domestic Intelligence*, Brennan Center for Justice, March 30, 2023, <https://www.brennancenter.org/our-work/policy-solutions/new-vision-domestic-intelligence>.

<sup>78</sup> E-Government Act of 2002 § 208(b)(1)(A).

<sup>79</sup> USCIS, USCIS-2025-0003-1240, 11.

<sup>80</sup> See DHS Privacy Office, *Privacy Impact Assessment for the Computer Linked Application Management System and Associated Systems (CLAIMS 3)*, June 30, 2020, <https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis016d-claims3-july2020.pdf>.

so with only passing reference to existing SORNs and PIAs that do not adequately cover use of social media handles—in clear violation of the law. The casual reference to DHS’s existing web of complex systems does not constitute meaningful or adequate notice to the public.

**d. DHS lacks oversight infrastructure to mitigate civil liberties and data breach risks.**

Finally, DHS does not have adequate internal or external oversight functions in place to ensure that civil liberties are safeguarded and data is protected against intentional or inadvertent misuse. This administration has pursued efforts to tear down internal oversight mechanisms and security infrastructure intended to protect civil liberties and secure its data holdings, which would include the social media identifiers it proposes to collect here. It has effectively shuttered DHS’s Office for Civil Rights and Civil Liberties and the Office of the USCIS Ombudsman, which are tasked with functions ranging from advising DHS on compliance with constitutional and other civil rights and liberties requirements to investigating complaints of abuses and helping people navigate problems that arise in the course of applying for immigration benefits.<sup>81</sup>

It has also gutted the Cybersecurity and Infrastructure Security Agency (CISA), which is tasked with protecting government systems from being compromised.<sup>82</sup> Indeed, major federal government database breaches are not uncommon, putting applicants’ anonymity and personal information at risk; one recent GAO report noted that federal agencies reported an average of 31,000 information security incidents between 2016 and 2022, and said that these attacks had become more “damaging and disruptive.”<sup>83</sup> When

---

<sup>81</sup> See, e.g., Economic Policy Institute, “Trump administration closes three DHS offices focused on civil rights and oversight,” April 3, 2025, <https://www.epi.org/policywatch/trump-administration-closes-three-dhs-offices-focused-on-civil-rights-and-oversight/>; and Ximena Bustillo, “Homeland Security makes cuts to civil rights and immigration oversight offices,” NPR, March 21, 2025, <https://www.npr.org/2025/03/21/nx-s1-5336738/homeland-security-rif-cuts-dhs>. Groups have filed lawsuits challenging the shuttering of these oversight offices. See Zach Montague and Hamed Aleaziz, “Lawsuit Aims to Reverse Firings at Internal Oversight Offices Within D.H.S.,” *New York Times*, April 24, 2025, <https://www.nytimes.com/2025/04/24/us/politics/lawsuit-firings-oversight-dhs.html>; and Robert F. Kennedy Human Rights v. U.S. Department of Homeland Security, No. 25-1270, (D.D.C. April 24, 2025). For an overview of what these oversight offices do and how they help mitigate DHS abuses, see Spencer Reynolds and Alia Shahzad,  *Holding Homeland Security Accountable*, Brennan Center for Justice, October 26, 2023, <https://www.brennancenter.org/our-work/policy-solutions/holding-homeland-security-accountable>.

<sup>82</sup> Kevin Collier, “‘Absolutely outraged’: Former cyber official targeted by Trump speaks out after cuts to U.S. digital defense,” NBC News, April 28, 2025, <https://www.nbcnews.com/politics/national-security/chris-krebs-speaks-cuts-trump-cuts-digital-defense-rcna203427>; and David 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/>.

<sup>83</sup> *Federal Agencies Need to Better Protect Sensitive Data: Testimony Before S. Subcomm. on Reg. Affairs & Fed. Management, S. Comm. on Homeland Security & Gov. Affairs, H. Subcomm. on Oversight &*

it comes to DHS records, concerning instances include a June 2019 hack that exposed tens of thousands of photos of drivers and license plates taken at border entry points.<sup>84</sup> People who may use social media to engage in political activism at the risk of retribution, for example, may be especially vulnerable if data they intend to keep private is exposed through a hack or otherwise becomes publicly available.

Even under the best of circumstances, DHS oversight has always been decentralized and inherently weak, leaving discretion for component agencies—such as USCIS—to develop their own oversight rules, or develop no rules at all. And there is no overarching office that would conduct oversight of intelligence activities like social media monitoring.<sup>85</sup>

### **III. The proposed collection does not meet the requirements of the PRA.**

Critically, the proposed collection does not satisfy the obligations of the PRA, which requires that an agency demonstrate that a proposed collection has “practical utility,” that it is not collecting information that is duplicative, and that complying with the proposed collection is not more burdensome than necessary.<sup>86</sup> For purposes of the PRA, “practical utility” is defined as information that is useful in fact rather than in theory, taking into account its “accuracy, validity, adequacy, and reliability,” along with the agency’s ability to process it in a “useful and timely fashion.”<sup>87</sup>

#### **a. DHS has failed to produce any evidence that the collection of social media identifiers to facilitate social media monitoring is an effective tool for screening and vetting immigrants, and it therefore lacks “practical utility.”**

Over nearly a decade, DHS has repeatedly failed to produce any evidence that the collection of social media identifiers to conduct social media monitoring facilitates better “vetting and national security screening” of immigrants.<sup>88</sup> Reviews of DHS’s social media screening have repeatedly and overtly called into question the practical utility, or “accuracy, validity . . . and reliability,” of information found on social media, and also described DHS’s inability to process it in a “useful and timely fashion.”

In 2021, government officials reviewing the use of social media to screen and vet people seeking entry into the United States acknowledged that it “add[ed] no value” to

---

*Management Efficiency, H. Comm. on Homeland Security*, 114th Cong., 4 (2015) (statement of Joel C. Willemsen, Managing Director, Information Technology), <https://www.gao.gov/assets/680/673678.pdf>.

<sup>84</sup> Zolan Kanno-Youngs and David E. Sanger, “Border Agency’s Images of Travelers Stolen in Hack,” *New York Times*, June 10, 2019, <https://www.nytimes.com/2019/06/10/us/politics/customs-data-breach.html>.

<sup>85</sup> See Reynolds and Shahzad, *Holding Homeland Security Accountable*.

<sup>86</sup> 5 C.F.R. § 1320.5(d)(1) (2025).

<sup>87</sup> 5 C.F.R. § 1320.3(l) (2025).

<sup>88</sup> See Collection Notice.

the process, and found that it had “very little impact on improving the screening accuracy of relevant systems.”<sup>89</sup> This sentiment echoes a 2016 transition brief prepared for the first Trump administration by DHS, which reported that in three out of its four social media screening pilots for refugees—who are among the individuals targeted by this proposed collection—“the information in [social media] 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.”<sup>90</sup> DHS did not identify any “derogatory information” on people screened pursuant to the fourth refugee pilot.<sup>91</sup> DHS also noted that it was difficult to discern the “authenticity, veracity, [and] social context” of social media content, as well as “whether the content evidences indicators of fraud, public safety, or national security concern.”<sup>92</sup>

It is unsurprising, then, that DHS officials concluded that “mass social media screening” was a poor use of resources: “[t]he process of social media screening and vetting necessitates a labor intensive manual review,” taking people away from “the more targeted enhanced vetting they are well trained and equipped to do.”<sup>93</sup>

Other internal DHS documents from 2016 and 2017 also indicate that pilot programs within USCIS were flawed. According to these documents, USCIS social media vetting provided little by way of actionable information.<sup>94</sup> By contrast, DHS concluded that such screening was “time and labor intensive”; that officers did not have clear guidance on what information was “potentially derogatory and worth further investigation”; and that “derogatory information found in other government systems can provide a more

---

<sup>89</sup> Charlie Savage, “Visa Applicants’ Social Media Data Doesn’t Help Screen for Terrorism, Documents Show,” *New York Times*, October 5, 2023, <https://www.nytimes.com/2023/10/05/us/social-media-screening-visa-terrorism.html> (citing documents obtained by The New York Times via Freedom of Information Act requests in which officials acknowledge that “there is little value” in collecting social media identifiers).

<sup>90</sup> The proposed collection includes changes to the I-590 form, which is filled out by those applying for refugee status. The new form would direct those applying to be refugees to submit their social media identifiers from the past five years. USCIS, USCIS-2025-0003-1239, DHS, September 17, 2025, <https://www.regulations.gov/document/USCIS-2025-0003-1239> (the proposed I-590 form); and USCIS, “USCIS Presidential Transition Records,” DHS, December 12, 2016, 198–199, <https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf> (hereinafter “USCIS Transition Records”).

<sup>91</sup> USCIS Transition Records, 199.

<sup>92</sup> USCIS Transition Records, 201.

<sup>93</sup> USCIS Transition Records, 201–202.

<sup>94</sup> Manar Waheed, New Documents Underscore Problems of ‘Social Media Vetting’ of Immigrants, ACLU (January 3, 2018), <https://www.aclu.org/blog/privacy-technology/internet-privacy/new-documents-underscore-problems-social-media-vetting>.

complete picture of the applicant’s background and risk profile” than social media.<sup>95</sup>

Likewise, a 2017 privacy compliance review found that DHS had not developed an adequate system to collect data that would “demonstrate the value of social media information to the VWP [Visa Waiver Program] application process,” including with respect to determining a traveler’s eligibility to enter the United States and evaluating whether the traveler posed a security risk.<sup>96</sup> And because it had only anecdotal success stories, not reliable data, it also could not adequately demonstrate that it was “collect[ing] the minimum PII [personally identifiable information] necessary” for the program, another key element in the PRA analysis.<sup>97</sup>

These conclusions turned on the same finding: that DHS relied on a small number of anecdotes to illustrate the efficacy of social media screening, which did “not constitute a reliable, effective system for the tracking and analysis of qualitative data” that would be needed to support claims of efficacy.<sup>98</sup> One of the review’s three recommendations was that DHS set up such a process incorporating comprehensive metrics—for example, how often social media information was proven to be inaccurate or contradicted information provided by the applicant—to measure the viability and success of social media screening.<sup>99</sup> It is unclear to what degree DHS has implemented this recommendation or to what extent it would apply it to the proposed collection. Even if it has been implemented, DHS has not provided any such holistic evidence of efficacy to the public, including in support of any proposal to collect social media for travel and immigration screening purposes.

In short, every one of DHS’s publicly available findings regarding the utility of social media monitoring as a tool to screen immigrants and travelers indicates that the administration has failed to demonstrate that its benefits outweigh its costs, and the collection of social media identifiers for these purposes thus cannot be justified.

---

<sup>95</sup> Fraud Detection and National Security Directorate, USCIS, *Review of the Defense Advanced Research Projects Agency 2.0 Social Media Pilot*, DHS, June 2, 2016, 33–34, 46, available at <https://s3.documentcloud.org/documents/4341532/COW2017000400-FOIA-Response.pdf> (hereinafter “USCIS, *Review of the Defense Advance Research*”).

<sup>96</sup> Privacy Office, DHS, *Privacy Compliance Review of the U.S. Customs and Border Protection Electronic System for Travel Authorization*, October 27, 2017, 8, <https://www.dhs.gov/sites/default/files/publications/CBP-ESTA%20PCR%20final%20report%2020171027.pdf>. Eligible people apply for visa-free travel to the United States using the Electronic System for Travel Authorization.

<sup>97</sup> Privacy Office, *Privacy Compliance Review*, 8.

<sup>98</sup> Privacy Office, *Privacy Compliance Review*, 8.

<sup>99</sup> Privacy Office, *Privacy Compliance Review*, 3.

**b. The proposed collection is duplicative of information DHS already has and is burdensome to comply with.**

The proposed collection is duplicative and unnecessarily burdensome: DHS already has access to and uses reams of information on people that bear on their legal eligibility for immigration benefits and whether they pose a security risk. As set forth above, the collection of social media identifiers also imposes serious costs to speech, association, anonymity, privacy, and due process.

Consider a person who initially comes to the United States on an employment visa, eventually becomes a permanent resident, and then applies for U.S. citizenship. If she applied for a visa in 2019 or after, she already would have supplied her social media identifiers on her visa application forms. She also would have provided a wealth of other information, some of it several times over, including addresses she has resided at; her travel history; her employment and educational history; information on her parents, her spouse or former spouse, and her children; answers to a litany of questions related to security and criminal history; biometric data, such as photographs and fingerprints; in-person responses to government officials during interviews about her application and documents; materials from her employer supporting her application, as relevant; and her social security number (which can be obtained with a work visa or green card).<sup>100</sup>

At each stage of the immigration process, the government may formally request more information beyond what is required to be provided on any application—for example, documents (e.g., birth certificates, other government records, or private records) or sworn testimony to corroborate claims.<sup>101</sup> And in addition to materials provided by the

---

<sup>100</sup> See, e.g., USCIS, Form DS-160 ("Nonimmigrant Visa Application"), DHS, available at <https://ceac.state.gov/genniv/>; USCIS, Form I-485 ("Application to Register Permanent Residence or Adjust Status"), DHS, available at <https://www.uscis.gov/sites/default/files/document/forms/i-485.pdf>; USCIS, Form I-129 ("Petition for a Nonimmigrant Worker"), DHS, available at <https://www.uscis.gov/sites/default/files/document/forms/i-129.pdf>; USCIS, I-140 ("Immigrant Petition for Alien Worker"), DHS, available at <https://www.uscis.gov/sites/default/files/document/forms/i-140.pdf>; and USCIS, Form N-400 ("Application for Naturalization"), DHS, available at <https://www.uscis.gov/sites/default/files/document/forms/n-400.pdf>. DHS also has the authority to "require and collect biometrics from any applicant, petitioner, sponsor, beneficiary, or other individual residing in the United States for any immigration and naturalization benefit." See USCIS, "Preparing for Your Biometric Services Appointment," DHS, July, 6, 2023, <https://www.uscis.gov/forms/filing-guidance/preparing-for-your-biometric-services-appointment>. See also USCIS, "USCIS to Expand In-Person Interview Requirements for Certain Permanent Residency Applicants," DHS, August 28, 2017, <https://www.uscis.gov/archive/uscis-to-expand-in-person-interview-requirements-for-certain-permanent-residency-applicants>.

<sup>101</sup> 8 CFR § 103.2 (2025). With respect to visa applications, under § 221(g) of the Immigration and Nationality Act, a consular officer can deny a visa application because he did not have all of the information required to conclude an applicant is eligible to receive a visa. In these cases, further documentation may be required. 8 U.S.C. § 1201(g). See also Bureau of Consular Affairs, U.S. Department

applicant, DHS has access to voluminous data—including social media data, travel records, and both domestic and international biometric and law enforcement databases, for example—that it can further use to try to identify security risks or test representations a person makes about their background and identity.<sup>102</sup>

It is thus no surprise that government officials have found that social media data offers little screening value, a point mentioned repeatedly and explicitly in internal assessments. As referenced above, such evaluations have noted that other data accessible to DHS “can provide a more complete picture of the applicant’s background and risk profile,” and that social media had “very little impact on improving the accuracy” of screening processes.<sup>103</sup>

As a result, the proposed collection, which would offer expanded access to applicants’ social media data, imposes an unnecessary burden on the public because it is not “necessary for the proper performance of the agency’s functions.”<sup>104</sup> And that extra paperwork burden is not insignificant. DHS’s estimate that it will take most applicants approximately forty minutes to fill out the social media question is likely an undercount, given that answering the question requires a person to think through and remember, for example, every platform they have used in the last five years and every possible identifier they have used on each of those platforms, including business or organizational accounts. The proposed collection’s vague and broad definition of social media exacerbates that burden.<sup>105</sup> People also regularly make accounts to use social media anonymously, which they may have trouble remembering when answering the proposed question.<sup>106</sup>

In some cases, the proposed collection would require applicants to include social

---

of State, “Visa Denials,” accessed October 16, 2025, <https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/visa-denials.html>.

<sup>102</sup> See, e.g., U.S. Customs and Border Protection (hereinafter CBP), DHS, *OIT Fiscal Year 2020 Year in Review*, March 6, 2025, 24–25, [https://www.cbp.gov/sites/default/files/2025-03/fy20\\_yir\\_1\\_final.pdf](https://www.cbp.gov/sites/default/files/2025-03/fy20_yir_1_final.pdf) (through the Automated Targeting System – Global (ATS-G), DHS has “increased CBP’s information sharing posture and cooperative relationship with [four] foreign countries”); Rachel Levinson-Waldman and Jose Guillermo Gutierrez, *Overdue Scrutiny for Watch Listing and Risk Prediction*, Brennan Center for Justice, October 19, 2023, <https://www.brennancenter.org/our-work/policy-solutions/overdue-scrutiny-watch-listing-and-risk-prediction>; and Harsha Panduranga et al., *Extreme Vetting & The Muslim Ban*, Brennan Center for Justice, October 7, 2017, [https://www.brennancenter.org/sites/default/files/publications/extreme\\_vetting\\_full\\_10.2.pdf](https://www.brennancenter.org/sites/default/files/publications/extreme_vetting_full_10.2.pdf).

<sup>103</sup> Savage, “Visa Applicants’ Social Media Data Doesn’t Help Screen for Terrorism, Documents Show”; and USCIS, *Review of the Defense Advance Research*.

<sup>104</sup> 5 C.F.R. 1320.5(d) (2025).

<sup>105</sup> See section II.c., *supra*. See also USCIS, USCIS-2025-0003-1247, DHS, September 17, 2025, 9, <https://www.regulations.gov/document/USCIS-2025-0003-1247> (the proposed N-400 form instructions).

<sup>106</sup> Serena Tara, “Study Finds Many New Yorkers Have Alts, Finstas, & Other Fake Social Accounts,” *Thrillist*, August 10, 2022, <https://www.thrillist.com/news/new-york/new-york-third-highest-number-alts-burner-accounts>.

media identifiers of relatives—including parents and stepparents, children, and even former spouses—likely a time-consuming process for applicants and their relatives.<sup>107</sup> Even if the applicant took the initiative to try to find the information themselves, it may be challenging or even impossible to find out whether someone has an account on a given platform, particularly if the platform does not require a name to sign up.

Moreover, the time frame for which people would be required to submit social media handle information is longer than, and untethered to, the period relevant to the benefits sought. For example, Form I-751 (“Petition to Remove Conditions on Residence”) is filed to upgrade a conditional two-year green card to a full ten-year one, if the person obtained the conditional green card through a marriage that was less than two years old.<sup>108</sup> DHS seeks to require disclosure of social media handles used over the five prior years, even though the main purpose of having people fill it out is to confirm that the marriage continued over the prior two years and was not entered into simply to obtain a green card. DHS provides no rationale for why this extended period is necessary.

#### **IV. A generic clearance for this set of collections is inappropriate.**

Finally, the category used for this proposal is inapt. DHS seeks approval of this set of collections pursuant to a “generic clearance,” meaning that it will be eligible to receive expedited OMB approval on each covered individual collection when DHS would normally have to seek separate approvals.

According to OMB, use of the “generic clearance” process is appropriate for “collections that are voluntary, low burden . . . and uncontroversial.”<sup>109</sup> Website satisfaction surveys, focus groups to address customer service issues, and prize competitions and contests are among those listed as “sample generic clearances.”<sup>110</sup> This approval process is wholly inappropriate for a substantive and weighty policy change in the collection of social media handles from more than three million people each year—including U.S. persons and their relatives—with the stated purposes of bolstering national security and enforcing immigration laws. The proposed collection is vastly more significant than, for example, a voluntary customer service survey of the National Park

---

<sup>107</sup> See, e.g., USCIS, USCIS-2025-0003-1232, DHS, September 17, 2025, <https://www.regulations.gov/document/USCIS-2025-0003-1232> (the proposed I-730 form); and USCIS, USCIS-2025-0003-1234.

<sup>108</sup> USCIS, Form I-751 (“Petition to Remove Conditions on Residence”), DHS, available at <https://www.uscis.gov/sites/default/files/document/forms/i-751.pdf>.

<sup>109</sup> Memorandum from Cass R. Sunstein, Administrator of the Office of Information and Regulatory Affairs, to the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, Re “Paperwork Reduction Act – Generic Clearances” (May 28, 2010), 2, [https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/inforeg/PRA\\_Gen\\_ICRs\\_5-28-2010.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/inforeg/PRA_Gen_ICRs_5-28-2010.pdf) (hereinafter “Memorandum from Sunstein”).

<sup>110</sup> Memorandum from Sunstein at 5.

Service to get information about visitors' trips, which was cited by OMB as an example of a long-running general clearance and does not come with adverse consequences for a failure to answer.<sup>111</sup>

First, the collections are not voluntary. Second, the collection of social media handles is not “low burden.” While DHS estimates that most people filling out the proposed social media question will spend forty minutes filling it out, that is—as we detail above—a low estimate, given the lack of clarity surrounding the precise requirements, the difficulty of remembering the extent of one’s online activity, and the requirement to obtain the same information from third parties. Characterizing that burden as “low” strains credulity.

Lastly, this proposal is anything but uncontroversial. In this comment, we highlight a number of aspects of the proposal that implicate the core constitutional rights that underpin a free and open society. Indeed, when the State Department proposed to collect social media identifiers from visa applicants, it received more than ten thousand public comments, many of which raised those same concerns.<sup>112</sup>

Pursuing a “generic clearance” for such a contested proposal with serious impacts on constitutional rights, including those of U.S. citizens, is wholly inappropriate and does not properly account for the scope or significance of the information sought.

## **V. Conclusion**

For the above reasons, we urge the Office of Management and Budget to deny the Department of Homeland Security’s proposed collection. If we can provide any further information regarding our concerns, please do not hesitate to reach out to Rachel Levinson-Waldman, Director, Liberty and National Security Program, Brennan Center for Justice, at [levinsonr@brennan.law.nyu.edu](mailto:levinsonr@brennan.law.nyu.edu), or Carrie DeCell, Senior Staff Attorney & Legislative Advisor, Knight First Amendment Institute, at [carrie.decell@knightcolumbia.org](mailto:carrie.decell@knightcolumbia.org).

Sincerely,

Brennan Center for Justice at NYU School of Law

Knight First Amendment Institute at Columbia University

---

<sup>111</sup> Memorandum from Sunstein at 6.

<sup>112</sup> Department of State, *Supporting Statement for Paperwork Reduction Act Submission: Electronic Application for Immigrant Visa and Alien Registration*, OMB Number 1405-0182, DS-160 and DS-156, April 11, 2019, 3, <https://www.reginfo.gov/public/do/DownloadDocument?objectID=85743802>.