Department of Homeland Security, U.S. Citizenship and Immigration Services

May 5, 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 oppose 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, or the "Department"), U.S. Citizenship and Immigration Services (USCIS).[1]

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.[2] In a stark departure from current policy, many of the people whose social media identifiers the Department 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.[3]

In April 2021, OMB rejected a proposal that included the same request to collect social media identifiers on the forms at issue here.[4] 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

[1] New Collection: Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms, 90 Fed. Reg. 11324 (March 5, 2024), https://www.federalregister.gov/documents/2025/03/05/2025-03492/agency-information-collection-activities-new-collection-generic-clearance-for-the-collection-of (hereinafter "Collection Notice").

[2] See Collection Notice. The notice estimates that the total number of respondents will be 3,574,983. For examples of forms that would solicit social media handles from third parties, see, e.g., United States Citizenship and Immigration Services (hereinafter USCIS), USCIS-2025-0003-0030, Department of Homeland Security (hereinafter "DHS"), March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0030 (the proposed I-751 form), and USCIS, USCIS-2025-0003-0034, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0034 (the proposed I-829 form).

[3] Previously, both the Departments of State and Homeland Security's collection of social media identifiers on visa forms 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-2025-0003-0030, and USCIS, USCIS-2025-0003-0008, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0008 (the proposed I-131 form).

[4] 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 (hereinafter "OMB Conclusion Re: ICR 202007-1601-001").

"practical utility" of collecting social media identifiers on these forms.[5] 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.[6]

The Department 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 social costs, such as the risks it poses to 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. For one, the Department's published notice says it is necessary to comply with Executive Order 14161, which—among other things—establishes a policy of screening people already in the United States for "hostile attitudes" and "hateful ideology."[7] These are phrases of the type that the administration regularly uses to label political positions with which it disagrees.[8] In April of this year, USCIS released statements indicating it would look for "antisemitic activity on social media," as well as "anti-Americanism," as grounds for denying immigration applications.[9] Across a range of perspectives on the current conflict in the Middle East, observers acknowledge that the administration uses "combating antisemitism" as a fig leaf for targeting constitutionally protected speech supportive of Palestine and/or critical of Israel.[10]

---

[5] 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.").

[6] OMB Notice of Action Re: ICR 202007-1601-001.

[7] Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats, 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.

[8] 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.

[9] 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#:~:text=In%20the%20first%20100%20days,with%20other%20agencies%2C%20helped%20reduce; 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.

[10] 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-antimsietim-executive-order-free-speech. Moreover, conservative and libertarian commentators alike have expressed

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, a broad and diverse coalition of organizations have repeatedly opposed the federal government's collection and screening of social media information on a number of grounds, including the chilling of free expression and association, the intrusiveness, and the disparate deployment and impact of these practices.[11] Our concerns about these damaging impacts only grow with the proposed extension of these practices to U.S. citizens and residents, and in an environment where people increasingly rely on social media as a primary channel for self-expression, organizing, and engaging with politics.

The DHS proposal plainly does not meet the requirements of the PRA, as OMB has previously found. Even setting aside the proposed collection's legal problems—which include serious constitutional deficiencies, of which a holistic discussion is outside the scope of these comments—it cannot be justified as sound policy. We write to urge the Department to abandon this proposal.

---

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.

[11] See, e.g., 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; 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-Visa%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-%2051817_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.

I. The proposed collection does not meet the requirements of the PRA.

For purposes of the PRA, federal regulation defines "practical utility" 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."[12] In addition to showing a proposed collection has "practical utility," the agency must also demonstrate that it is not collecting information that is duplicative, and that complying with the proposed collection is not more burdensome than necessary.[13]

a. DHS has failed to produce any evidence that 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 social media monitoring facilitates better "identity verification, national security and public safety screening" of immigrants.[14]

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 the process, and found that it had "very little impact on improving the screening accuracy of relevant systems."[15]

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."[16] The Department did not identify any "derogatory information" on people screened pursuant to the fourth refugee pilot.[17] 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."[18] 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."[19]

---

[12] 5 C.F.R. § 1320.3(l) (2025).
[13] 5 C.F.R. § 1320.5(d)(1) (2025).
[14] See Collection Notice.
[15] 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).
[16] 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-2025-0003-0022, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0022 (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").
[17] USCIS Transition Records, 199.
[18] USCIS Transition Records, 201.
[19] USCIS Transition Records, 201–202.

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.[20] By contrast, the Department 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 complete picture of the applicant's background and risk profile" than social media.[21]

A 2017 report by the DHS Office of the Inspector General examined six social media monitoring programs piloted by USCIS and Immigration and Customs Enforcement (ICE) to screen applicants for immigration benefits. The Inspector General found that "these pilots, on which DHS plans to base future department-wide use of social media screening, lack criteria for measuring performance to ensure they meet their objectives."[22] Since the Department did not methodically evaluate these pilots to determine whether they performed well or poorly, the Inspector General concluded that they could not serve to justify scaling social media monitoring on a DHS-wide basis: exactly what the Department proposes to do here.[23]

Likewise, a 2017 privacy compliance review found that DHS could not "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.[24] Nor could it demonstrate that the collection of social media handles minimized the burdens on VWP applicants by "collect[ing] the minimum PII [personally identifiable information] necessary" to vet them.[25]

Both of 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.[26] 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.[27] It is unclear to what degree DHS has

---

[20] 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.

[21] 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*").

[22] Office of Inspector General (hereinafter OIG), *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted)*, February 27, 2017, 2, https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.

[23] OIG, *DHS' Pilots for Social Media Screening*, 7.

[24] 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.

[25] Privacy Office, *Privacy Compliance Review*, 8.

[26] Privacy Office, *Privacy Compliance Review*, 8.

[27] Privacy Office, *Privacy Compliance Review*, 3.

implemented this recommendation. And even if it has been implemented, the Department 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 the Department's publicly available findings regarding the utility of social media monitoring as a tool to screen immigrants and travelers indicates that the proposed collection does not meet the PRA requirements. The documents discussed above repeatedly and overtly call into question the practical utility, or "accuracy, validity…and reliability," of information found on social media, and also describe the inability of the Department to process it in a "useful and timely fashion." Crucially, any value the Department claims that social media has is fully conjectural—"merely [] theoretical or potential" at very best, rather than "actual" or proven, as the PRA requires.[28]

b. The proposed collection is duplicative of information the Department 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.

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, which raises its own constitutional concerns. She also would have provided a wealth of other information, some of it several times over, including addresses she has resided at, along with 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 security and criminal-history related questions; 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).[29]

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

[28] 5 C.F.R. § 1320.3(l) (2025).

[29] 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; 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.

corroborate claims.[30] And in addition to materials provided by the 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.[31]

Given so, it is no surprise that government officials have found that social media data offers little marginal 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.[32]

As a result, the proposed collection imposes an unnecessary burden on the public because it is not "necessary for the proper performance of the agency's functions."[33] And that extra paperwork burden is not insignificant. The Department's estimate that it will take less than five minutes to fill out the social media question strains credulity, 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. People also regularly make accounts to use social media anonymously, which they may have trouble remembering to disclose when answering the proposed question.[34]

In some cases, the proposed collection would require applicants to include social media identifiers of relatives—including parents and stepparents, children, and even former spouses—likely a time-consuming process for applicants and their relatives.[35] 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

---

[30] 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 of State, "Visa Denials," last accessed April 28, 2025, https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/visa-denials.html.

[31] 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 (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.

[32] Savage, "Visa Applicants' Social Media Data Doesn't Help Screen for Terrorism, Documents Show"; and USCIS, *Review of the Defense Advance Research*.

[33] 5 C.F.R. 1320.5(d) (2025).

[34] 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.

[35] See, e.g., USCIS, USCIS-2025-0003-0025, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0025 (the proposed I-730 form); and USCIS, USCIS-2025-0003-0034, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0034 (the proposed I-829 form).

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.[36] 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.

II. The proposed collection harms core constitutional rights.

The proposed collection undermines the rights to speech, association, anonymity, privacy, and due process, all of which are guaranteed by the U.S. Constitution. The fact that many of the people from whom social media identifiers would be sought are U.S. citizens, permanent residents, or 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 occurred, in the absence of any showing of criminal or other prohibited activity, and using tools ill-suited to the assessment of threats.

We underscore that non-U.S. citizens in the United States have constitutional rights, given their presence in and connections to the country, as internal government legal analyses have acknowledged.[37] They may retain these constitutional rights even when they are outside the country, depending on whether they have legal status and the strength of their U.S. contacts.[38] This proposal thus implicates the constitutional rights of nearly everyone it touches.

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."[39] Consequently, for many people—indeed, for many Americans—the proposed collection will inhibit speech and activity in one of the primary ways

[36] 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.

[37] 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/tgj1if1nii. 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").

[38] ICE, DHS, Memorandum re Inadmissibility, 4–5.

[39] Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017).

they may choose to connect with the world around them. In essence, people affected by the collection—including Americans—have a choice they should not have to make: either risk retaliation for their online activity or self-censor.

Impact on Speech

This administration has declared that it is retaliating against people for their political speech. On his first day in office, the president issued an executive order—which the Department cites to justify the proposed collection—directing agencies to propose steps to protect Americans from people who have "hostile attitudes" towards American "citizens, culture, government, institutions, or founding principles."[40] Further, USCIS has, for example, said it is screening people's social media for "Anti-American activity" when adjudicating immigration applications.[41] These are undefined phrases that echo language regularly aimed at political opponents and could encompass a range of First Amendment-protected speech.

Additionally, with the stated aim of combating antisemitism, DHS has set up a task force that scours the social media histories of foreign students in the United States to search for evidence of their involvement in pro-Palestine and/or anti-Israel protests.[42] In high-profile cases such as those of Mahmoud Khalil and Rümeysa Öztürk, the government has cited expressions of political views as a key—if not the sole—basis for barring an individual otherwise here lawfully from staying in the country.[43]

These actions have created a climate in which people applying for immigration benefits—with their future in the United States at stake—may be unlikely to risk speaking out on a topic that could be considered even mildly controversial, knowing that their social media activity may be monitored.

---

[40] Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats, Exec. Order No. 14161, 90 Fed. Reg. 8451.

[41] See, e.g., USCIS, "First 100 Days."

[42] 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; 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; and "International Student Visas Revoked," Inside Higher Ed, April 7, 2025, https://www.insidehighered.com/news/global/international-students-us/2025/04/07/where-students-have-had-their-visas-revoked.

[43] In its initial court filings in its case against Khalil, the government cited 8 U.S.C. § 1227(a)(4)(C)(i), a provision rendering a noncitizen deportable if the Secretary of State the authority "has reasonable ground to believe" that the individual's "presence or activities" "would have potentially serious adverse foreign policy consequences for the United States." 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. In support of this provision, the government has not accused Khalil of any criminal activity, instead relying on a memo signed by Secretary of State Marco Rubio which said that it is U.S. foreign policy to "combat anti-Semitism around the world and in the United States, in addition to efforts to protect Jewish students from harassment and violence in the United States." See Lauren Mascarenhas and Gloria Pazmino, Newly-released memo from Rubio details government's only evidence in effort to deport Mahmoud Khalil, CNN, April 10, 2025, https://www.cnn.com/2025/04/10/us/mahmoud-khalil-evidence-deadline/index.html. The government is relying on the same foreign policy provision in its case against Öztürk. First Amendment Petition for Writ of Habeas Corpus and Complaint at 8, Öztürk v. Trump, No. 25-cv-10695 (D. Mass. March 28, 2025). According to a DHS spokesperson, Öztürk had engaged in "activities in support of Hamas," presumably referring to an op-ed she co-wrote for a school newspaper criticizing her university's response to calls to divest from companies with ties to Israel. Gloria Pazmino et al., "What we know about the Tufts University PhD student detained by federal agents," CNN, March 28, 2025, https://www.cnn.com/2025/03/27/us/rumeysa-ozturk-detained-what-we-know/index.html.

In addition, 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—and these misinterpretations can have serious consequences.[44] Last year, in a particularly shocking 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.[45] Elon Musk's social media posts related to the financial condition and share price of Tesla have become 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.[46] Additional examples illustrate the point.[47]

If the Department 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 consequent chilling effects on speech are not conjectural. Social media monitoring, like other forms of surveillance, impacts what people say, what they hear, and with whom they interact online.[48] The proposed collection, if approved, will pressure people—including many

[44] 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. See also Complaint for Declaratory and Injunctive Relief at 23–24, No. 19-3632, (D.D.C. December 5, 2019) (explaining how difficult it can be to interpret social media posts "without a nuanced understanding of the context in which they are made").

[45] 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.

[46] 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.

[47] See, e.g., 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.

[48] 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

Americans—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 of misinterpretation or adverse consequences. An ongoing lawsuit filed by the Brennan Center and the Knight First Amendment Institute against the State Department and DHS documents these impacts in a nearly identical context;[49] so too does a recent lawsuit led by the Knight First Amendment Institute challenging 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.[50]

Our objections to social media monitoring apply with equal force to speech across the political spectrum. During the Biden presidency, allies of Donald Trump made similar objections, articulating concerns about the impacts on free expression raised by the prior administration's surveillance and mining of social media.[51]

Use of Automated Tools Amplifies Risks to Free Expression

According to recent reporting, DHS is also expanding the use of automated tools to analyze social media posts, and it is likely that those tools will be directed at posts and other data associated with the social media identifiers it seeks through the proposed collection.[52] For years, the Brennan Center and other organizations have explained that these tools are not reliable because, among other things, they have biases reflecting those in their training data; they cannot properly account for context; and they often perform poorly when they are asked to translate non-English languages.[53] We do not fully re-expound on those concerns here. But we provide some more recent examples of the use of automated tools to screen or moderate content—whether by the government or technology companies—that show how these issues persist today, and have even been magnified.

For instance, the administration has recently used keyword searches to flag content as part of

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.

[49] Brennan Center for Justice, "Case Tracker: Doc Society v. Blinken," updated May 1, 2024, https://www.brennancenter.org/our-work/court-cases/doc-society-v-blinken.

[50] See generally American Association of University Professors v. Rubio, No. 25-cv-10685 (D. Mass. March 25, 2025).

[51] See, e.g., Rep. Jim Jordan to Christopher A. Wray (director, Federal Bureau of Investigation), Re: FBI Facebook Tool, November 12, 2024, https://nypost.com/wp-content/uploads/sites/2/2024/11/FBI_Facebook_Tool.pdf; see also Jacyln Diaz, "FBI Director Wray grilled as House GOP members allege 'politicization' of the agency," NPR, July 12, 2023, https://www.npr.org/2023/07/12/1186993033/fbi-director-house-hearing-christopher-wray; and Heritage Foundation, "Oversight Project Sues Biden DHS for Documents on Federal Surveillance of Americans' Social Media Accounts," press release, July 7, 2022, https://www.heritage.org/press/oversight-project-sues-biden-dhs-documents-federal-surveillance-americans-social-media.

[52] 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."

[53] 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.

its efforts to purge programs and references related to "DEI" [Diversity, Equity, and Inclusion] from the federal government, and ended up making a number of glaring errors—failing to account for obvious context, sometimes with significant consequences. It mistakenly put on leave a federal employee who managed relationships with businesses held by private equity, because of the inclusion of the term "equity."[54] 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.[55] 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 word "gay."[56]

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.[57]

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.[58] For this reason, the use of such technology to identify wrongdoing, such as plagiarism or other lower-level misdeeds, has been controversial, given the consequences for the accused.[59] The stakes are far higher for people seeking U.S. citizenship or affirming permanent residency for their spouse, necessitating scrupulous accuracy and transparency.

Notwithstanding these known shortfalls, a January 2025 Inspector General report evaluating DHS's oversight of its use of artificial intelligence found that the department "did not have adequate governance process to monitor AI compliance with privacy and civil rights and civil liberties requirements," suggesting that it is not equipped to systematically identify and mitigate these substantial risks.[60]

---

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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/.

[59] See, e.g., Christopher Beam, "The AI Detection Arms Race Is On," *WIRED*, September 14, 2023, https://www.wired.com/story/ai-detection-chat-gpt-college-students/; Geoffrey A. Fowler, "What to do when you're accused of AI cheating," *Washington Post*, August 14, 2023, https://www.washingtonpost.com/technology/2023/08/14/prove-false-positive-ai-detection-turnitin-gptzero/; and Miles Klee, "Professor Flunks All His Students After ChatGPT Falsely Claims It Wrote Their Papers," *RollingStone*, May 17, 2023, https://www.rollingstone.com/culture/culture-features/texas-am-chatgpt-ai-professor-flunks-students-false-claims-1234736601/.

[60] Joseph V. Cuffari, OIG, OIG-25-10: Final Report: DHS Has Taken Steps to Develop and Govern Artificial

Impact on Association

The proposed rule would open the door to ongoing online surveillance of U.S. persons, including citizens, legal permanent residents, and others physically present in the country. In addition to the social media identifiers of the applicants themselves, the Department also explicitly seeks from applicants the social media identifiers of third-party relatives whose relationship may be relevant to the benefit sought.

On some forms included in the proposal, such as I-751 ("Petition to Remove Conditions on Residence"), DHS would explicitly require people applying for benefits to disclose the social media handles of their US citizen relatives who are not seeking benefits or services requiring government scrutiny, though it fails to make this point clear in its regulatory notice.[61] Other forms solicit social media handles from legal permanent residents, such as the N-400 ("Application for Naturalization"), and from people living or present in the United States, such as the I-485 ("Application to Register Permanent Residence or Adjust Status").[62] In requiring the disclosure of U.S. persons' social media identifiers to the federal government, even when they are not themselves applying for an immigration benefit, the proposed collection represents a major departure from current policy, which raises its own constitutional concerns, but only requires this information directly from visa applicants outside the United States.

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. 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. This is true even if their identifiers are not explicitly disclosed by the applicant—and even if they are U.S. citizens who would have no reason to believe the U.S. government would be scrutinizing their social media activity.

Applicants are also at risk of being held accountable for what people they have interacted with say or do. 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 student had neither written nor engaged with them.[63]

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 other immigration benefit. 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

---

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.

[61] USCIS, USCIS-2025-0003-0030, and USCIS, USCIS-2025-0003-0008, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0008 (the proposed I-131 form).

[62] USCIS, USCIS-2025-0003-0037, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0037 (the proposed N-400 form); USCIS, USCIS-2025-0003-0013, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0013 (the proposed I-485 form).

[63] 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.

residence, for instance, is estimated to be approximately two years.[64]

Impact on Anonymous Speech

The rights to communicate anonymously and associate privately are protected by the First Amendment.[65] "[A]n author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment."[66] 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."[67] However, 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.[68] By compelling applicants to disclose any social media identifiers they have used on social media platforms during the preceding five years—including pseudonymous identifiers—the proposed collection unquestionably burdens the applicants' First Amendment right to speak anonymously online.

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 forms.[69]

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,

---

[64] USCIS, "Historical National Median Processing Time (in Months) for All USCIS Offices for Select Forms By Fiscal Year," DHS, accessed May 3, 2025, https://egov.uscis.gov/processing-times/historic-pt.

[65] 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," last accessed April 28, 2025, https://www.eff.org/issues/anonymity.

[66] McIntyre, 514 U.S. at 342.

[67] NAACP, 357 U.S. at 462.

[68] 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)." Neither the instructions to applicants nor the supporting materials for the proposed collection offer a definition of "social media," suggesting that certain more privacy-focused applications that do not require users to create a handle—such as Signal, Telegram, or WhatsApp—could conceivably be covered. 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. In any event, the broad framing in this respect 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.

[69] *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 v. Pompeo, 19-cv-03632 (D.D.C. May 28, 2020), https://knightcolumbia.org/documents/4b2d5c21ad.

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 thing—putting them in the uncomfortable 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.

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 uncloaking 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 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.[70] 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 they "collect[] in one place many distinct types of information … that reveal much more in combination than any isolated record."[71] 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 harmless – practices.[72] 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.

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,

[70] 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.

[71] 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.

[72] 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)).

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.

Social media can also reveal more about a person than they intend to reveal. 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, 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.[73] Taken together with the expansive retention and dissemination policies that we discuss below, a person could even be exposed to serious risk by handing over their identifiers to DHS: location data and inferences drawn from other posts, for example, could reveal a visit to a family planning clinic, risking criminal punishment as abortion becomes functionally illegal in some states.

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 being able to comply is contingent on the cooperation of third parties.

None of the instructional materials accompanying the relevant forms defines "social media," only giving non-exhaustive lists of examples such as "Facebook, X, Instagram, etc."[74] This 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. The Department provides even less guidance than what accompanied the State Department's collection on visa forms—which at least specified a range of platforms for which disclosure was required, although it left ambiguous whether platforms not listed were not covered.[75]

In asking applicants to compile the identifiers of relatives, the proposed requirement also makes them susceptible to a third party's faltering accuracy or memory. The applicant is asked to

[73] 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.
[74] See, e.g., USCIS, USCIS-2025-0003-0030.
[75] State Department, "Frequently Asked Questions on Social Media Identifiers in the DS-160 and DS-260," June 4, 2019, https://travel.state.gov/content/dam/visas/Enhanced%20Vetting/CA%20-%20FAQs%20on%20Social%20Media%20Collection%20-%206-4-2019%20(v.2).pdf (noting that "A social media "handle" or "identifier" is any name used by the individual on social media platforms including, but not limited to, Facebook, Twitter, and Instagram. The updated visa application forms list the specific social media platforms for which identifiers are being requested."). An online example of the DS-160 form shows the full list of social media identifiers to choose from. See Bureau of Consular Affairs, *Online Nonimmigrant Visa Application: DS-160, Exemplar*, Department of State, November 1, 2019, 19 https://www.tahirih.org/wp-content/uploads/2020/02/DS-160-Example_11012019.pdf.

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, or may have an incentive to withhold information they don't want the applicant to know.

Particularly alarming, DHS wants to collect the social media identifiers of applicants' minor children, without any mention of protocols governing the review, privacy, and security of such information.[76] 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 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.[77] We have also documented these issues in the context of social media surveillance in U.S. schools.[78]

Ultimately, we are concerned that a failure to comply with the proposed collection, even inadvertently, may be used as a pretext 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, the Department must clarify in far greater detail what is necessary to comply with the requirements of this proposed collection.

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

The Department 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.[79] Further, this 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

[76] See, e.g., the proposed changes to the I-751 form, which ask for the social media identifiers of the applicant's children. USCIS, USCIS-2025-0003-0030.

[77] 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.

[78] Brennan Center for Justice, "Schools: Social Media Surveillance," accessed April 25, 2025, https://www.brennancenter.org/issues/protect-liberty-security/social-media/schools-social-media-surveillance.

[79] 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. 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.

in the United States, with functionally no oversight to mitigate the concomitant data privacy and civil liberties risks.[80]

DHS Policies Enable Ongoing Surveillance of U.S. Persons

DHS maintains an official record of an individual's visa and immigration history in an Alien File (A-File) that is stored for 100 years after the individual's date of birth.[81] A-Files contain social media information like "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, even though the government could not otherwise compel citizens to disclose their social media identifiers. 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 the Department'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.[82]

By enabling the long-term retention of social media-related data, the proposed collection 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.[83] 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.[84] By contrast, it is not at all clear what, if any, limitations USCIS intends to apply in the first instance. Downstream, as noted above, DHS claims the authority to share the identifiers it has collected broadly and indefinitely.

The Proposed Collection Violates the Privacy Act

The maintenance of records such as social media handles is governed by the Privacy Act, and

---

[80] 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.

[81] DHS-2017-0038 SORN at 43561.

[82] DHS-2017-0038 SORN at 43557. 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.

[83] 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.

[84] 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.

the proposal is insufficient to comply with 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.[85] The Privacy Act incorporates key principles, known as the Fair Information Practice Principles, or FIPPs, and includes the ability for the public to determine what records pertaining to them are collected, maintained, used, or disseminated by an agency. It also requires agencies to collect such records only for lawful and authorized purposes and safeguard them appropriately.[86]

The notice proposing the collection of social media handles does not satisfy 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 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."[87]

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."[88] 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 "relevant and necessary" information, maintain "accurate, relevant, timely, and complete records," or "establish safeguards" for protecting the information.[89]

Indeed, 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.[90] As we highlight throughout this comment, information about the First Amendment-protected activities of citizens and legal 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 relating to political beliefs, association, and religion.

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.[91] The social media handle proposal

[85] *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.
[86] 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.
[87] See Collection Notice.
[88] USCIS, USCIS-2025-0003-0031, DHS, March 5, 2025, 10, https://www.regulations.gov/document/USCIS-2025-0003-0031 (the proposed I-751 form instructions).
[89] 5 U.S.C. §§ 522(a)(e)(1), (5), (10) (2025).
[90] 5 U.S.C. § 522(a)(e)(7) (2025).
[91] 5 U.S.C. § 522(a)(e)(4) (2025).

does not purport to establish a new system of records; instead, it indicates that it will use the social media records in accordance with existing SORNs. Existing SORNs do not adequately explain how social media handles will be collected, stored, or disclosed, however. 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.[92]

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 members.[93] The A-Files SORN only allows for maintenance of records for "relatives and associates of any of the individuals listed above who are "subject to" the Immigration and Nationality Act. Many family members will be outside that scope.[94] The Immigration Biometric and Background Check SORN does not explicitly provide for maintenance of social media handles at all.[95]

DHS Fails to Assess Privacy Risks of the Proposed Collection

DHS also has ceased conducting programmatic privacy impact assessments that would assess the privacy risks related to these proposed changes and is now only conducting privacy impact assessments required by the E-Government Act of 2002, which requires federal agencies to ensure sufficient privacy protections of personal information. In particular, the E-Government Act requires agencies to conduct PIAs when initiating a new collection of information.[96]

Despite the breadth of DHS's current proposal, DHS also has not conducted a privacy impact assessment (PIA) that complies with the E-Government Act. Although DHS's social media notice will result in the collection of new information—including information about lawful permanent residents and citizen family members—DHS has not published a PIA and has not 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.[97] But the CLAIMS PIA does not even reference collection of social media handles for family members, let alone provide sufficient detail about how their social media handles and those of applicants will be evaluated when considering eligibility for an immigration

[92] USCIS, USCIS-2025-0003-0031, 11; and 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.
[93] See USCIS, USCIS-2025-0003-0030, and USCIS, USCIS-2025-0003-0035, DHS, March 5, 2025, https://www.regulations.gov/document/USCIS-2025-0003-0035; 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-securityus-citizenship-and.
[94] DHS-2017-0038 SORN at 43559.
[95] DHS-2018-0003.
[96] E-Government Act of 2002 § 208(b)(1)(A).
[97] USCIS, USCIS-2025-0003-0031, DHS, March 5, 2025, 11, https://www.regulations.gov/document/USCIS-2025-0003-0031.

benefit.[98]

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

Lack of Oversight Infrastructure to Mitigate Civil Liberties and Data Breach Risks

Finally, 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 the Department'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, investigating complaints of abuses, and helping people navigate problems they are having in the course of applying for immigration benefits.[99]

It has also gutted the Cybersecurity and Infrastructure Security Agency (CISA), which is tasked with protecting government systems from being compromised.[100] 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."[101] When 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.[102] People who may use social media to engage in political activism at

---

[98] 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.

[99] 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/; 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.

[100] 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/.

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

[102] 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.

the risk of retribution, for example, may be especially vulnerable if data they intend to keep private 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.[103]

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

Finally, we conclude with another regulatory point. 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 the Department 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."[104] Website satisfaction surveys, focus groups to address customer service issues, and prize competitions and contests are among those listed as "sample generic clearances."[105] 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 the immigration laws. The proposed collection is vastly more significant than, for example, a voluntary customer service survey of the National Park 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.[106]

First, the collections are not voluntary. Second, the collection of social media handles is not "low burden."[72] While DHS estimates that people filling out the proposed social media question will spend four minutes filling it out, that is—as we detail above—a very 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 Department of State proposed to collect social media identifiers from visa applicants, it received more than ten thousand public comments, many of which raised those same concerns.[107]

---

[103] See Reynolds and Shahzad, *Holding Homeland Security Accountable*.

[104] 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 (hereinafter "Memorandum from Sunstein").

[105] Memorandum from Sunstein at 5.

[106] Memorandum from Sunstein at 6.

[107] 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.

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 significance of the information sought.

V. Conclusion

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

Sincerely,

Brennan Center for Justice at NYU School of Law

Knight First Amendment Institute at Columbia University