Department of Homeland Security

November 4, 2019

Re: Agency Information Collection Activities: Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms (Docket Number DHS-2019-0044)

Dear Sir or Madam:

The undersigned organizations write to urge the Department of Homeland Security (DHS) to withdraw the Department's proposed rule, published at Docket Number DHS-2019-0044, to require disclosure of social media identifiers from certain people seeking to travel or be admitted to the United States, or who are applying for immigration-related benefits, including those who are already living in the country.[1]

Civil, human, and immigrant rights organizations have repeatedly opposed the federal government's collection and screening of social media information, and raised concerns about the chilling effect on speech, intrusion into privacy, and disparate impact of the government's policies, as well as the government's discriminatory deployment of this practice.[2]

Below, we enumerate the risks associated with the the Department's proposed rule to collect and use applicants' social media information as part of its vetting processes, and call upon DHS to retract this rule.

---

[1] 84 Fed. Reg. 46557 - 46561 (posted Sept. 4, 2019), *available at* https://www.federalregister.gov/d/2019-19021.

[2] *See, e.g.,* Comments of the Brennan Center, *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; Comments of the Brennan Center, *Application for Nonimmigrant Visa & Electronic Application for Immigrant Visa and Alien Registration, OMB Control No. 1405-185* (Sept. 27, 2018), https://www.brennancenter.org/sites/default/files/analysis/OIRA%20Letter_9.27.2018.pdf; Comments of the Electronic Privacy Information Center, *Supplemental Questions for Visa Applicants* (Dec. 27, 2017), https://epic.org/EPIC-DOS-Visas-SocialMediaID-Dec2017.pdf; Comments of Center for Democracy & Technology, *Coalition Letter Opposing DHS Social Media Retention* (Oct 18, 2017), https://cdt.org/insight/coalition-letter-opposing-dhs-social-media-retention/; Comments of the Brennan Center, *Supplemental Questions for Visa Applicants* (Oct. 2, 2017), https://www.brennancenter.org/sites/default/files/StateDeptcomments-10.2.2017.pdf; Comments of the ACLU, *Supplemental Questions for Visa Applicants* (Oct. 2, 2017), https://www.aclu.org/letter/aclu-comment-supplemental-questions-visa-applicants; Comments of the Brennan Center, *Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants* (May 18, 2017), https://www.brennancenter.org/sites/default/files/State%20Dept%20Information%20Collection%20Comments%20-%2051817_3.pdf; Comments of the Brennan Center, *Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization* (Aug. 22, 2016), https://www.brennancenter.org/our-work/research-reports/brennan-center-submits-comments-dhs-plan-collect-social-media-information.

I. **The proposed rule raises significant constitutional concerns and jeopardizes fundamental human rights principles.**

A system that penalizes people or subjects them to enhanced monitoring for their speech raises significant constitutional concerns and will likely violate the civil rights and liberties of millions of people, including those living in the United States.

A. The proposed rule undermines the First Amendment.

Requiring applicants for immigration benefits to provide their social media identifiers will chill the exercise of their First Amendment rights to free speech, anonymity, and free association.

Social media platforms are a crucial place for modern public discourse. Billions of people use social media to share news or ideas, connect with others, and to spur social or political change. As the U.S. Supreme Court noted recently, 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."[3] The proposed rule will thus inhibit a range of speech and activity from the millions of people that it will affect every year.

The deleterious effects of surveillance on free speech have been well documented in empirical research.[4] Social media monitoring, like other forms of surveillance, impacts what people say,

---

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

[4] Elizabeth Stoycheff et al., *Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects*, 21 NEW MEDIA & SOCIETY 1-18 (2018), https://journals.sagepub.com/doi/abs/10.1177/1461444818801317. *See also* Dawinder S. Sidhu, *The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans*, 7 U. MD. L.J. RACE RELIG. GENDER & CLASS 375 (2007), https://core.ac.uk/download/pdf/56358880.pdf; Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMMUNICATION QUARTERLY 296–311 (2016), https://journals.sagepub.com/doi/ pdf/10.1177/1077699016630255. Similarly, in a survey of a representative sample of U.S. internet users, 62 percent reported that they would be much less or somewhat less likely to touch on certain topics if the government was watching, with 78 percent of respondents agreeing that they would be more cautious about what they said online. J. W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6 INTERNET POLICY REVIEW (2017), https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case. Another study measured how internet users in 11 countries reacted when they found out that DHS was keeping track of searches of terms that it regarded as suspicious, such as "state of emergency" and "drug war." Users were less likely to search using terms that they believed might get them in trouble with the U.S. government. Alex Marthews and Catherine Tucker, *Government Surveillance and Internet Search Behavior*, February 17, 2017, https://ssrn.com/abstract=2412564. The study analyzed the search prevalence of select keywords compiled by the Media Monitoring Capability section of the National Operations Center of DHS. The list of keywords was publicized in 2012 as "suspicious" selectors that might lead to a particular user being flagged for analysis by the National Security Agency (NSA). *See* DHS, National Operations Center Media Monitoring Capability, *Analyst's Desktop Binder*, 20, https://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf. The authors later expanded their study to 41 countries and found that, for terms that users believed might get them in trouble with the U.S. government, the search prevalence fell by about 4 percent across the countries studied. Alex Marthews and Catherine Tucker, *The Impact of Online Surveillance on Behavior, in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 446 (David Gray and Stephen E. Henderson, ed. 2017). *See also* HUMAN RIGHTS WATCH, WITH LIBERTY TO MONITOR ALL: HOW LARGE-SCALE U.S. SURVEILLANCE IS HARMING JOURNALISM, LAW, AND

what they hear, and with whom they interact online. One recent 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.[5] Even people who said they had nothing to hide were highly likely to self-censor online when they knew the government was watching.[6] The proposed rule may pressure applicants to engage in self-censorship like deleting their accounts, disassociating with online connections, limiting their social media postings, or sanitizing their internet presence for fear of reprisal.

The collection of social media information will also undermine the right to communicate anonymously, which is protected by the First Amendment.[7] On certain social media platforms, like Reddit, it is common for users to create "throwaway" accounts, which are accounts users may not associate with their identities in order to remain anonymous.[8] For example, users from countries where it is physically dangerous to identify as lesbian, gay, bisexual, or transgender (LGBT) might create a throwaway account to protect their identity while interacting with the LGBT community online. Similarly, political activists facing retribution or harm in their home countries may use pseudonymous social media identifiers to protect themselves from having their identity linked to their online speech. Under the proposed rule, those who use pseudonymous identifiers will be required to surrender their anonymity as a condition of obtaining immigration benefits.

The proposed rule also undermines free association. It will discourage individuals, including U.S. persons, from making connections on social media because they reasonably fear those ties will be subject to misinterpretation or retaliation, as described in Section II.A. Moreover, Americans may not be able to associate with their friends, business associates, relatives or other contacts who would otherwise visit or immigrate to the U.S. but do not wish to provide their social media information.

B. The proposed rule is an excessive invasion of privacy.

Collecting information about an individual's social media accounts is inherently more invasive than gathering information like a phone number or address. A phone number will result in a

---

AMERICAN DEMOCRACY (July 28, 2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and.

[5] Stoycheff et al., *Privacy and the Panopticon*; Sidhu, *The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans*.

[6] Stoycheff, *Under Surveillance*, 307-8.

[7] *See e.g.,* 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."); *Anonymity*, ELECTRONIC FRONTIER FOUNDATION, accessed September 27, 2017, https://www.eff.org/issues/anonymity. *See also* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep., Human Rights Council, at 1, U.N. Doc. A/HRC/29/32, May 22, 2015, *available at* http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

[8] Alex Leavitt, *This is a Throwaway Account,* 18 ACM CONF. ON COMPUTER SUPPORTED COOPERATIVE WORK & SOCIAL COMPUTING PROC. 317-327 (2015), https://dl.acm.org/citation.cfm?id=2675175.

specific and static data point, whereas having access to someone's social media accounts will enable DHS to conduct a historical, ongoing, and prospective review of their online activity.

Moreover, much more information is available about a person from their social media presence than may be apparent at first glance, or than they intend to share. For example, in a recent study, researchers accurately predicted where Twitter users – many of whom did not know they had shared their location – lived, worked, prayed, or spent time out at night based on geolocation data embedded in their tweets.[9] The dragnet nature of this collection, anticipated to affect 33 million people, only makes its impact worse. The more data the government has on applicants – indeed, it intends to "maintain a record of persons applying for specific immigration and other travel benefits" – the more connections it can draw between them, and the more it may know about any one person's familial, social, and professional life and the lives of her contacts, even if she has stopped or limited her use of social media.[10]

C. The proposed rule will result in increased monitoring of the speech and activity of those living in the United States.

Given the breadth of information that can be deduced from an individual's social media profile, the proposed rule will greatly expand the Department's intrusion into the speech and privacy of those seeking immigration benefits while living in United States.

While existing social media monitoring programs target visa applications,[11] the proposed rule would subject United States persons with lawful immigration status, including Legal Permanent Residents (LPRs), to social media vetting. DHS seeks to collect social media identifiers from LPRs seeking to naturalize (Form N-400), remove conditions on their residence (Form I-751), or travel (Form I-131).

The proposed rule will also result in DHS monitoring the friends, family members, business associates, and acquaintances of those living in the United States — regardless of their immigration status — because social media is inherently interactive. A review of an individual's social media page necessarily encompasses not only their speech, but also the speech of anyone who has shared, commented, liked, or reposted to their page. The rule will likely chill the speech of U.S. citizens and residents corresponding with friends or relatives seeking entry into the United States. Consider, for example, how an American citizen who wants her brother in Iraq to visit or emigrate might think twice before posting tweets criticizing U.S. policy or remaining Facebook friends with someone who does.[12] Additionally, this information might be shared or used by other agencies or their components, such as the Federal Bureau of Investigation (FBI), Immigration and Customs

---

[9] 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.

[10] James P. Bagrow, Xipei Lui, & Lewis Mitchell, *Information flows reveals prediction limits in online social media activity*, NATURE HUMAN BEHAVIOR 122-128 (2019), https://arxiv.org/pdf/1708.04575.pdf.

[11] 83 Fed. Reg. 13,806 (Mar. 30, 2018); 83 Fed. Reg. 13,807 (Mar. 30, 2018).

[12] *See*, e.g. Karen Zraick & Mihir Zaveri, *Harvard Student Says He Was Barred From U.S. Over His Friends' Social Media Posts*, N.Y. TIMES (Aug. 27, 2019), https://nyti.ms/2ZvMJ93.

Enforcement (ICE), or even local law enforcement, amplifying these constitutional issues, as discussed in Section III.

Troublingly, recent reports and government disclosures have indicated that DHS is already actively conducting social media monitoring of American citizens, signifying that the Department does not view Americans' speech as warranting protection from government intrusion. In March, reports surfaced that the Department was engaging in social media tracking of American journalists and immigration advocates at the border.[13] In May, the Acting Secretary of Homeland Security issued a memorandum providing that the Department has the authority to monitor and retain information on U.S. citizens and legal permanent residents in their exercise of protected First Amendment activities, such as religious practice or protest of government policies, "when that activity is relevant to the granting or denial of a pending application."[14] This effectively nullifies the Privacy Act's bar on maintaining records of U.S. persons' First Amendment-protected activity – to which the DHS notice perfunctorily refers.[15] Because the proposed rule claims to relate directly to "the granting or denial of a pending application," there is a high risk that information about the First Amendment-protected activities of citizens and LPRs – collected via social media as well as other mechanisms – could be incorporated into applicants' files or even result in repercussions from other government agencies.

D. The proposed rule conflicts with the International Covenant on Civil and Political Rights.

The proposed rule is also incongruent with the International Covenant on Civil and Political Rights, which the United States has ratified. The ICCPR guarantees "the right to freedom of expression," including the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[16] As described in the preceding sections, requiring applicants to provide their social media identifiers may have deleterious effects on free speech and chill the exercise of freedom of association and anonymity.

II. Social media monitoring is subjective, will capture unreliable and circumstantial evidence, and will likely result in arbitrary, ineffective, and inconsistent determinations.

---

[13] Tom Jones, Mari Payton & Bill Feather, *Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database*, NBC 7 SAN DIEGO, Mar. 6, 2019, https://www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html.

[14] Memorandum from Kevin K. McAleenan, Acting Sec'y, Dep't of Homeland Sec., to All DHS employees, "Information Regarding First Amendment Protected Activities," May 17, 2019, 2, https://www.dhs.gov/sites/default/files/publications/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019.pdf

[15] 84 Fed. Reg. 46557, 46559; *see also* The Privacy Act of 1974, 5 U.S.C.A. § 552a.

[16] International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Exec. Rep. 102-23, 999 U.N.T.S. 171, https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf

Social media data has known limitations as an effective vetting tool. Communications on social media can be easily misconstrued by both human reviewers and analytical programs. In fact, DHS's own review of its social media monitoring pilot programs did not find a sufficient basis to justify scaling the practice. To the extent that DHS will attempt to use social media information to predict national security threats, there are no reliable indicators for that purpose.

A. Communication on social media is easily misinterpreted and misattributed.

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.[17] In 2012, for instance, a British national was denied entry at a Los Angeles airport when DHS agents misinterpreted his posting on Twitter that he was going to "destroy America" (slang for partying) and "dig up Marilyn Monroe's grave" (a joking reference to a television show).[18] In another example, an American police department's efforts to unearth bomb threats online instead turned up references to "bomb" (i.e., excellent) pizza.[19]

Non-verbal communications – including shares, likes, favorites, and retweets – pose additional challenges, as they do not have a universally agreed-upon meaning. For instance, someone might "like" a comment on Facebook to call attention to a post, to get notifications about a comment thread, as an endorsement, to express sympathy, or because they want to follow a brand, celebrity, or politician, even one with whom they vehemently disagree.

The possibility that online speech might be misinterpreted is magnified when the speech is in a language other than that spoken by the reviewer. In an internal list of challenges for its existing social media pilot programs, DHS noted that "[c]ontent obtained from social media is often in languages other than English and requires translation support"[20] – this is no surprise when travelers and immigrants to the U.S. may come from more than 190 countries speaking more than 7,000 languages – but there is little showing that the Department has the necessary translation support services to review the social media communications of such a diverse population.[21] Indeed, an

---

[17] *See, e.g.*, Natasha Lennard, *The Way Dzhokhar Tsarnaev's Tweets Are Being Used in the Boston Bombing Trial Is Very Dangerous*, FUSION (Mar. 12, 2015), http://fusion.net/story/102297/the-use-of-dzhokhar-tsarnaevstweets-in-the-bostonbombing-trial-is-very-dangerous/; Bill Chappell, *Supreme Court Tosses Out Man's Conviction for Making Threat on Facebook*, NATIONAL PUBLIC RADIO (June 1, 2015), http://www.npr.org/sections/thetwo-way/2015/06/01/411213431/supreme-court-tosses-outman-s-conviction-formaking-threats-on-facebook.

[18] *See* J. David Goodman, *Travelers Say They Were Denied Entry to U.S. for Twitter Jokes*, N.Y. TIMES (Jan. 30, 2012), https://thelede.blogs.nytimes.com/2012/01/30/travelers-say-they-were-denied-entry-to-u-s-for-twitter-jokes.

[19] 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-regularly-yielded-false.

[20] USCIS BRIEFING BOOK, 184.

[21] One widely cited estimate is that there are about 7,111 living languages, of which 3,995 have a developed writing system. *See* ETHNOLOGUE: LANGUAGES OF THE WORLD (David M. Eberhard et al. eds., 22nd ed. 2019), https://www.ethnologue.com/enterprise-faq/how-many-languages-world-are-unwritten-0. The Department of State issues nonimmigrant visas to individuals from every country in the world annually. *See* DEPARTMENT OF STATE, REPORT OF THE VISA OFFICE 2018, TABLE XVIII: "NONIMMIGRANT VISAS ISSUED BY NATIONALITY

internal manual produced by U.S. Citizenship and Immigration Services (USCIS) directs agents to first use free online translation services like "Google, Yahoo, Bing, and other search engines" when analyzing non-English social media content, suggesting the agency does not have the resources to conduct in-person translation services for the data it is collecting.[22]

Under the proposed rule, DHS will analyze not only an applicant's online speech, but also their network of social media contacts and the speech of their contacts. This creates further opportunities for misinterpretation. Social media platforms generate visible connections between individuals, but do not differentiate whether the connection is between family, friends, business associates, or acquaintances.[23] On Facebook, for example, all contacts are designated as "friends" regardless of the intimacy or strength of their relationship.[24] Examining content from the social media pages of an applicant's contacts increases the risk of relying on information that in no way reflects on the applicant's beliefs or activities.

A Customs and Border Protection agent, for example, recently turned away a Palestinian student traveling from Lebanon to study at Harvard University because, after searching through the student's social media account, the agent "found people posting political points of view that oppose the U.S. on [the student's] friend list." The student himself had no political posts on his own timeline and had never liked, shared, or commented the flagged posts. (And even if he had, political views should not be the basis for the denial of one's entry into the country.) Only after significant outcry from Harvard and the public did DHS, days later, allow the student to enter the United States and begin school.[25]

B. Automated screening tools do not provide reliable or objective assessments of social media communications.

DHS seeks to require over 33 million people to provide their social media identifiers for almost 20 different platforms over the previous five years. Given the volume of information DHS intends to collect, it is likely the Department will turn to automated tools to assist with analysis of social media content. While the full scope of DHS's efforts to use algorithms is not known, research

---

(INCLUDING BORDER CROSSING CARDS) FISCAL YEAR 2009–
2018," https://travel.state.gov/content/dam/visas/Statistics/AnnualReports/FY2018AnnualReport/FY18AnnualRepor
t%20-%20TableXVIII.pdf.

[22] Yeganeh Torbati, *Google Says Google Translate Can't Replace Human Translators. Immigration Officials Have Used It to Vet Refugees*, PROPUBLICA (Sept. 26, 2019), https://www.propublica.org/article/google-says-google-translate-cant-replace-human-translators-immigration-officials-have-used-it-to-vet-refugees.

[23] Nicole B. Ellison & danah m. boyd, *Sociality Through Social Network Sites*, *in* THE OXFORD HANDBOOK OF INTERNET STUDIES (Jan. 2013) (noting social media platforms create "a publicly visible, personally curated list of contacts" but that Facebook users report about 25–30 percent of their total Facebook Friends are "actual" friends).

[24] J. Donath & danah boyd, *Public Displays of Connection*, 22 BT TECH. J. 71, 72 (2004), https://smg.media.mit.edu/papers/Donath/PublicDisplays.pdf (discussing how the links on most networking sites are unnuanced, meaning "there is no distinction made between a close relative and a near stranger one chatted with idly on-line one night.").

[25] Karen Zraick & Mihir Zaveri, *Harvard Student Says He Was Barred From U.S. Over His Friends' Social Media Posts*, N.Y. TIMES (Aug. 27, 2019), https://nyti.ms/2ZvMJ93; Joshua Rhett Miller, *Deported Harvard Student Ismail Ajjawi Arrives At University For Start Of Classes*, N.Y. POST (Sept. 3, 2019), https://nypost.com/2019/09/03/deported-harvard-student-ismail-ajjawi-arrives-at-university-for-start-of-classes/.

shows that at least three branches of DHS — Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and USCIS — now use automated processes to analyze social media information, either alongside other data or by itself.[26]

Existing algorithmic tools used to analyze text are widely recognized to have large error rates. Studies show that top-rated natural language processing tools, which are commonly used to judge the meaning of text, have an error rate of 20 to 30 percent.[27] Algorithmic tone and sentiment analysis, which senior DHS officials have suggested is being used to analyze social media,[28] is even less accurate. Accuracy plummets even further when the speech being analyzed is not standard English. Translation services like Google Translate and others frequently misinterpret or mistranslate social media profiles because of the prevalence of slang, abbreviations, and unstandardized grammar in social media posts.[29] Indeed, Google itself advises that Google Translate is not "intended to replace human translators," casting serious doubt on why USCIS has nevertheless instructed agents to use it and other similar services.[30]

C. Social media monitoring programs have not proven effective.[31]

DHS has failed to provide any evidence that social media monitoring works in support of the proposed collection. A 2017 report by the Office of the Inspector General, examining six social media monitoring programs piloted by DHS, 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."[32] Since the Department did not methodically evaluate these

---

[26] FAIZA PATEL, RACHEL LEVINSON-WALDMAN, SOPHIA DenUYL, & RAYA KOREH, SOCIAL MEDIA MONITORING 7 (Brennan Center for Justice 2019), https://www.brennancenter.org/sites/default/files/2019-08/Report_Social_Media_Monitoring.pdf; *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted)*, OFFICE OF INSPECTOR GENERAL, 5 (quoting a memo from the DHS Under Secretary for Intelligence and Analysis dated December 29, 2016 stating: "at the launch of the task force, neither the private sector nor the U.S. Government possessed the capabilities for large-scale social media screening...DHS has made strides in identifying and assessing social media screening technology and conducting pilots that will enable the development of such capabilities."); USCIS BRIEFING BOOK, 183 (noting "FDNS, a part of the DHS Social Media Task Force, continues to collaborate with partner components and agencies to explore semi-automated solutions").

[27] *See e.g.*, Malmasi & Zampieri, *Challenges in Discriminating Profanity From Hate Speech,* 1-16; Kwok & Wang, *Locate the Hate*; Han, *Improving the Utility of Social Media With Natural Language Processing*.

[28] *See* Aaron Cantú & George Joseph, *Trump's Border Security May Search Your Social Media by 'Tone'*, THE NATION (Aug. 23, 2017), https://www.thenation.com/article/trumps-border-security-may-search-your-social-media-by-tone/.

[29] Torbati, *Google Says Google Translate Can't Replace Human Translators*; *see also* Su Lin Blodgett & Brendan O'Connor, *Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English*, FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY IN MACHINE LEARNING CONF. PROC. 2 (2017), https://arxiv.org/pdf/1707.00061.pdf (noting that one tool flagged posts in English slang as Danish with 99.9 percent confidence).

[30] Torbati, *Google Says Google Translate Can't Replace Human Translators*.

[31] *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted)*, OFFICE OF INSPECTOR GENERAL; *USCIS Social Media & Vetting: Overview and Efforts to Date*, U.S. CITIZENSHIP AND IMMIGRATION SERVICES (Mar. 2, 2017), https://assets.documentcloud.org/documents/4341532/COW2017000400-FOIA-Response.pdf#page=56.

[32] *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted)*, OFFICE OF INSPECTOR GENERAL, 1.

programs to determine whether they performed well or poorly, the Inspector General concluded that they could not serve as a foundation to scale social media monitoring on a DHS-wide basis. Yet that is exactly what the Department is proposing to do here, even though it has not pointed to any subsequent tests or research concluding otherwise.

DHS has also internally questioned the efficacy of its social media monitoring pilot programs. In a brief from late 2016 prepared for the incoming administration, DHS reported that in three out of its four programs used to vet refugees – who are targeted by the 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."[33] 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."[34] 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."[35]

Documents from 2016 and 2017 also indicated that DHS pilots within USCIS were flawed.[36] According to these documents, USCIS social media vetting provided little by way of actionable information.[37] Instead—as feared by civil rights and liberties experts—this social media surveillance appeared to be without guidance, parameters, or results, underscoring the likelihood of unjust profiling and discrimination.[38]

D. There are no criteria or indictators to reliably predict criminal or terrorist acts.

DHS's notice specifies that social media may also be helpful in determining "previously unidentified national security or law enforcement concerns, such as when criminals and terrorists have provided otherwise unavailable information via social media, that identified their true intentions, including support for terrorist organizations."[39] However, to the extent that DHS will attempt to use social media information to predict national security threats, there are no reliable indicators for that purpose. According to researchers, there are no identified reliable criteria that

---

[33] USCIS BRIEFING BOOK, 181.

[34] *Id.* at 183.

[35] *Id*. at 183-4.

[36] Aliya Sternstein, *Obama Team Did Some 'Extreme Vetting' of Muslims Before Trump, New Documents Show,* DAILY BEAST (Jan. 2, 2018), https://www.thedailybeast.com/obama-team-did-some-extreme-vetting-of-muslims-before-trump-new-documents-show.

[37] Manar Waheed, *New Documents Underscore Problems of 'Social Media Vetting' of Immigrants,* ACLU (Jan. 3, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/new-documents-underscore-problems-social-media-vetting.

[38] U.S. Citizenship and Immigration Services, *Review of [Redacted] Adjustment of Status Social Media Pilots*, 8, *available at* https://assets.documentcloud.org/documents/4341532/COW2017000400-FOIA-Response.pdf#page=33 (In fact, one document states "If USCIS officers need to determine which social media records are potential national security concerns, and which are not, they will need training and clear guidance.").

[39] 84 Fed. Reg. 46557, 46558.

can predict who will commit a terrorist act.[40] Numerous empirical studies have concluded that a person's decision to engage in political violence is a complex one, involving myriad environmental and individual factors, none of which is necessary or sufficient in every case, and none of which falls into a linear path or process resulting in violence.[41]

Additionally, computers, like humans, are not equipped to identify indicators of terrorism or criminality. In response to the government's plans in 2017 to deploy automated decision-making tools to predict terrorism or other crimes, technologists and civil liberties experts pointed out that the use of those tools for that purpose would be both ineffective and discriminatory. They expressed "grave concern" that these methods could not provide objective assessments and would instead result in inaccurate and biased determinations.[42] Similarly, a coalition of civil rights and liberties, immigrant rights, and privacy organizations detailed their opposition to such a process, as it would be discriminatory, ineffective, and a threat to constitutional rights as well as civil rights and liberties.[43]

III. The proposed rule will exacerbate privacy concerns with DHS's existing practices regarding information sharing and retention.

DHS's notice provides few concrete limitations on the dissemination, retention, or storage of the data it will collect under this rule. After asserting that "[n]o assurance of confidentiality is provided," the notice states that "[a]ll data submitted under this collection will be handled in accordance with applicable U.S. laws and DHS policies regarding personally identifiable information."[44] Following this statement is a reference to the Privacy Act of 1974 and a laundry list of citations to additional laws, privacy guidance, policies, and privacy impact assessments.[45] However, the Privacy Act applies only to U.S. citizens and legal permanent residents. Even where the Privacy Act might apply (i.e., to information on U.S. persons), few protections are provided. The proposed rule lists a number of system of records "associated with this information collection."[46] Most, if not all, of these system of records notices exempt the data they contain from many of the protections of the Privacy Act. Additionally, the systems all have a long list of "routine uses" that allow for disclosures to a broad set of entities. The proposed rule will allow the social

---

[40] *See e.g.,* Decl. of Marc Sageman, *Latif v. Holder*, No. 3:10-cv-00750, 2015 WL 1883890 (D. Or. Aug 7, 2015), https://www.aclu.org/legal-document/latif-et-al-v-holder-et-al-declaration-marc-sageman; *See* JAMIE BARLETT, JONATHAN BIRDWELL, AND MICHAEL KING, THE EDGE OF VIOLENCE: A RADICAL APPROACH TO EXTREMISM (DEMOS 2010), https://www.demos.co.uk/files/Edge_of_Violence_-_web.pdf.

[41] SOCIAL SCIENCE FOR COUNTERTERRORISM: PUTTING THE PIECES TOGETHER (Paul K. Davis and Kim Cragin, eds., RAND National Defense Research Institute 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG849.pdf.

[42] Letter from 54 Technology Experts to Hon. Elaine Duke, Sec'y of Homeland Security (Nov. 16, 2017), https://www.brennancenter.org/sites/default/files/Technology%20Experts%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%2011.15.17.pdf.

[43] Brennan Center for Justice et al., to Hon. Elaine Duke, Sec'y of Homeland Security (Nov. 16, 2017), https://www.brennancenter.org/sites/default/files/Coalition%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%2011.15.17.pdf.

[44] 84 Fed. Reg. 46557, 46561.

[45] *Id.*

[46] *Id.*

media information to be collected in numerous databases while doing little to explain how the Department will use, store, or disseminate the data it obtains or how the harms of doing so will be mitigated.

Moreover, the retention of social media information amplifies the chilling effect of DHS's proposed collection on free speech, since applicants may reasonably believe they are being monitored at any time after they disclose their identifiers. DHS presumably intends to store the information it collects from visa applicants in its highly interconnected databases.[47] It is public knowledge that some of these databases have extremely long retention periods. For example, 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.[48] A-files contain social media information like "social media handles, aliases, associated identifiable information, and search results."[49] Additionally, the sensitive applicant information collected would likely be disclosed to the National Vetting Center, which coordinates the federal government's vetting functions and consolidates data streams with the goal of identifying "known or suspected threat actors" using "relevant indicators that inform adjudications and determinations related to national security, border security, homeland security, or public safety."[50] Under the proposed rule, DHS will certainly have the identifying information necessary to conduct ongoing surveillance of applicant's social media accounts, even after their application for an immigration benefit has been awarded or denied. The Department's long-term retention policies magnify the privacy intrusions of the proposed rule.

Lastly, there is a risk that the information collected under the proposed rule will be subject to data breaches, further exacerbating other harms. Major federal government database breaches are not uncommon, putting applicants' anonymity and personal information at risk. The federal government has been the victim of multiple data breaches in the recent past, with the number of breaches of government data rising sharply, from 5,503 to 67,168, between 2006 and 2014.[51] DHS has not been immune from this threat: a Government Accountability Office Report from 2015 found that the design and implementation of the Department's information security controls had significant flaws.[52] In June 2019, a hack of DHS records exposed tens of thousands of photos of drivers and license plates taken at border entry points.[53] For applicants using pseudonyms to communicate with a marginalized community in their home country or to engage in activism

---

[47] PATEL ET AL., SOCIAL MEDIA MONITORING, 12.

[48] 82 Fed. Reg. 43556 (posted Sept. 18, 2017), *available at* https://www.federalregister.gov/d/2017-19365.

[49] *Id.* at 43557.

[50] United States. The White House. Presidential Memorandum on Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise, available at https://www.whitehouse.gov/presidentialactions/presidential-memorandum-optimizing-use-federal-government-information-support-national-vettingenterprise/.

[51] *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., 1 (2015) (statement of Joel C. Willemssen, Managing Director, Information Technology), *available at* https://www.gao.gov/assets/680/673678.pdf.

[52] *Id.*

[53] Zolan Kanno-Youngs & David E. Sanger, *Border Agency's Images of Travelers Stolen in Hack*, N.Y. TIMES (June 10, 2019) https://www.nytimes.com/2019/06/10/us/politics/customs-data-breach.html.

online, a data breach might result in grave harm or retaliation. Moreover, the risk of a data breach aggravates the harm faced by individuals whose countries of origin criminalize the use of social media as this collection forces such applicants to identify and document their use of social media, and then hope that such admission does not make its way back to their country of origin.

IV.   The proposed rule opens the door for ideological vetting based on stereotypes, of Muslim communities in particular.

The proposed rule is linked to Executive Order 13780, the second in a sequence of "Muslim Ban" executive orders that have stopped people from a set of predominantly Muslim-majority countries from coming to the United States.

The first executive order was discriminatory on its face. In addition to containing a religious minority exemption for countries named in the Muslim ban – which President Trump admitted was intended to benefit Christians – it borrowed verbatim from a campaign speech by then-candidate Trump entitled "Understanding the Threat: Radical Islam and the Age of Terror," in which he called for a ban of visas from certain parts of the world and an ideological screening test for Muslims, among other things.[54] In that speech, Trump proposed that the United States admit only those "who share our values and respect our people,"[55] implying that Muslims do not. Campaign and administration officials have, more than once, said social media would be used to make these kinds of judgments.[56]

In response to pushback from courts,[57] the president and his advisers withdrew the first order but referred to its immediate successor – Executive Order 13780, the basis for the proposed collection – as a "politically correct" version that would accomplish the "same basic policy outcome."[58] Reviewing this second order, one federal court of appeals found that it "speaks with vague words of national security, but in context drips with religious intolerance, animus, and discrimination."[59] In this context, DHS's recitation of its policies and commitments related to

---

[54] Exec. Order No. 13,769, 82 Fed. Reg. 8977 (January 27, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-02-01/pdf/2017-02281.pdf.

[55] Jeremy Diamond, *Trump Proposes Values Test for Would-be Immigrants in Fiery ISIS Speech*, CNN (Aug. 15, 2016),
http://www.cnn.com/2016/08/14/politics/donald-trump-isis-fight/.

[56] *Donald Trump calls for 'extreme vetting' of immigrants and visitors to the U.S.*, CHICAGO TRIBUNE (Aug. 15, 2016), https://www.chicagotribune.com/nation-world/ct-donald-trump-terrorism-speech-20160815-story.html;
Laura Meckler, *Trump Administration Considers Far-Reaching Steps for 'Extreme Vetting'*, WALL STREET JOURNAL (Apr. 4, 2017), https://www.wsj.com/articles/trump-administration-considers-far-reaching-steps-for-extreme-vetting-1491303602; Laura Meckler, *For Trump Administration, 'Extreme Vetting' Has Wide Scope*, WALL STREET JOURNAL (Mar. 27, 2017), https://www.wsj.com/articles/for-trump-administration-extreme-vetting-has-wide-scope-1490621976.

[57] Mark Landler, *Appeals Court Rejects Request to Immediately Restore Travel Ban*, N.Y. TIMES (Feb. 4, 2017), https://www.nytimes.com/2017/02/04/us/politics/visa-ban-trump-judge-james-robart.html.

[58] Donald J. Trump, TWITTER, June 5, 2017, https://twitter.com/realdonaldtrump/status/871675245043888128 ("The Justice Dept. should have stayed with the original Travel Ban, not the watered down, politically correct version they submitted to S.C.").

[59] IRAP v. Trump, 857 F.3d 554, 572 (4th Cir. 2017) (en banc); see also Trump v. Int'l Refugee Assistance, 138 S. Ct. 353, 199 L. Ed. 2d 203 (2017) (remanding to the United States Court of Appeals for the Fourth Circuit with instructions to dismiss as moot the challenge). In a 5-4 ruling, the Supreme Court vacated preliminary injunctions

nondiscrimination and consistent treatment under the law in the course of seeking approval for this proposed collection ring hollow.[60]

Moreover, Muslim, Arab, Middle Eastern, and South Asian communities have historically been particularly vulnerable to targeting by U.S. government counterterrorism and surveillance programs,[61] including those involving social media screening specifically. For example, from 2002 to 2011, the National Security Entry-Exit Registration System (NSEERS) required young men from Muslim-majority countries to register when they entered the United States and regularly check in with immigration officials.[62] At least two of the USCIS social media monitoring pilot programs implemented near the end of the Obama administration only had Arabic translation capabilities, suggesting that they were also intended to target applicants from Arab countries.[63] One DHS pilot program specifically directed social media surveillance at refugees from both Iraq and Syria.[64] And in 2018, a prominent refugee organization reported that refugee applicants from mostly Muslim-majority countries were subjected to enhanced screening.[65] A leaked DHS draft report dated early 2018 similarly tagged young Muslim men as "at-risk persons" who should be subjected to intensive screening and ongoing monitoring.[66]

Policies should be based on proof, not prejudice. And while no proof has been offered that the proposed collection will enhance national security, there is plenty of evidence that prejudice has played a role in this administration's ratcheting up of vetting procedures. Indeed, writing in opposition to Executive Order 13780, more than 130 national security experts from across the political spectrum argued that vetting should be responsive to "specific, credible threats based on individualized information," not stereotypes of religions or countries.[67]

---

agianst the Trump administration's third Muslim ban in Trump v. Hawaii, 138 S. Ct. 2392, 201 L. Ed. 2d 775 (2018).

[60] 84 Fed. Reg. 46557, 46558–46569 (listing DHS and component agency policies related to bias and nondiscrimination).

[61] George Joseph, *Draft DHS Report Called for Long-Term Surveillance of Sunni Muslim Immigrants,* FOREIGN POLICY (Feb. 5, 2018), https://foreignpolicy.com/2018/02/05/draft-dhs-report-surveillance-of-muslim-immigrants; FAIZA PATEL, RETHINKING RADICALIZATION (Brennan Center 2011), www.brennancenter.org/sites/default/files/legacy/RethinkingRadicalization.pdf.

[62] Nadeem Muaddi, *The Bush-Era Muslim Registry Failed. Yet The US Could Be Trying It Again*, CNN (Dec. 22, 2016), https://www.cnn.com/2016/11/18/politics/nseers-muslim-database-qa-trnd/index.html (describing the National Security Entry-Exit Registration System, which required young men from Muslim-majority countries to register when they entered the US and regularly check in with immigration officials).

[63] *See* U.S. Citizenship and Immigration Services, *Review of the Defense Advanced Research Projects Agency 2.0 Social Media Pilot* (June 2, 2016) 9, https://www.documentcloud.org/documents/4341532-COW2017000400-FOIA-Response.html#document/p1; USCIS BRIEFING BOOK, 181.

[64] PATEL ET AL., SOCIAL MEDIA MONITORING, 30, 32.

[65] Laura Koran & Tal Kopan, *US Increases Vetting and Resumes Processing of Refugees From 'High-Risk' Countries*, CNN (Jan. 29, 2018), https://www.cnn.com/2018/01/29/politics/us-refugee-vetting-measures/index.html.

[66] *Demographic Profile of Perpetrators of Terrorist Attacks in the United States Since September 2001 Attacks Reveals Screening and Vetting Implications*, U.S. DEP'T OF HOMELAND SEC. (2018), https://assets.documentcloud.org/documents/4366754/Text-of-CPB-Report.pdf.

[67] Lara Jakes, *Trump's Revised Travel Ban Is Denounced by 134 Foreign Policy Experts*, N.Y. TIMES (Mar. 11, 2017), https://nyti.ms/2mck8ix (letter available at https://assets.documentcloud.org/documents/3515708/LetterFormerOfficialsonMarch6EO-Pdf.pdf).

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

DHS seeks regulatory approval of this set of collections pursuant to a "generic clearance," meaning that it will be eligible to receive expedited Office of Management and Budget (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."[68] Website satisfaction surveys, focus groups to address customer service issues, and prize competitions and contests are among those listed as "sample generic clearances."[69] This approval process is wholly inappropriate for the collection of social media handles from 33 million people – spanning everyone from visitors coming to the U.S. for a short stay to individuals who have lived here for years – with the alleged purposes of bolstering national security and enforcing the immigration laws.[70]

First, the collections are not voluntary. The Department characterizes the disclosure of social media identifiers as "mandatory" and notes that some online applications cannot be submitted unless a response to the question is recorded. While the disclosure of handles is not technically "required to obtain or retain a benefit," DHS says that "failure to provide the requested data may either delay or make it impossible…to determine an individual's eligibility for the requested benefit," meaning that not answering will hurt the applicant. This 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 does not come with adverse consequences for a failure to answer, and was cited by OMB as an example of a long-running general clearance.[71]

Second, the collection of social media handles is not "low burden," even if it does not take much text to answer.[72] DHS estimates, conservatively, that the roughly 33 million people from whom social media identifiers will be collected will spend over 12 million "burden hours" filling out the forms. Characterizing that burden as "low" strains credibility. Further, twenty handles are listed and the requirement goes back five years. People may not recall immediately, if at all, their handles on platforms that no longer exist or are infrequently used – for example, Vine or MySpace. People may also have had multiple accounts on a single platform over a half decade that they find difficult to recall.

Finally, this proposal is anything but uncontroversial. In this comment, we highlight a number of aspects of the proposal that implicate the core constitutional rights and human rights principles that are building blocks of 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

---

[68] 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, "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.

[69] *Id*. at 5.

[70] 84 Fed. Reg. 46557, 46561.

[71] Memorandum from Sunstein at 6.

[72] *Id*. at 2 (stating that "low-burden" is assessed "based on a consideration of total burden, total respondents, or burden per respondent").

comments, many of which raised those same concerns.[73] Much is at stake for applicants – not properly disclosing their social media identifiers could cost a person anything from missing a business trip to failing to qualify as a refugee or asylee when fleeing a war zone, or even being denied U.S. citizenship.[74]

VI. Conclusion.

For the above reasons, we urge the Department of Homeland Security to abandon this proposed information collection initiative. Please do not hesitate to let us know if we can provide any further information regarding our concerns. We may be reached at pandurangah@brennan.law.nyu.edu (Harsha Panduranga), mwaheed@aclu.org (Manar Waheed), mazarmi@cdt.org (Mana Azarmi), or jscott@epic.org (Jeramie Scott).

Sincerely,

American Civil Liberties Union (ACLU)
American Immigration Lawyers Association (AILA)
American-Arab Anti-Discrimination Committee (ADC)
Arab American Institute
Asian Americans Advancing Justice | AAJC
Asian Counseling and Referral Service (ACRS)
Boundless Immigration, Inc.
Brennan Center for Justice at NYU School of Law
Catholic Legal Immigration Network, Inc. (CLINIC)
Center for Democracy & Technology
Central American Resource Center (CARECEN DC)
Central American Resource Center of California (CARECEN LA)
Citizenshipworks
Coalition for Humane Immigrant Rights (CHIRLA)
Council on American-Islamic Relations
Defending Rights & Dissent
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)

---

[73] 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.

[74] Among other things, DHS seeks to collect social media identifiers from Legal Permanent Residents seeking to naturalize (Form N-400), remove conditions on their residence (I-819), or to travel (Form I-131). It proposed rule also applies to non-immigrant applicants for benefits like asylum (Form I–589), and to prospective travelers through the Electronic System for Travel Authorization (ESTA) and Electronic Visa Update System (EVUS).

Entre Hermanos
Free Press
HIAS Pennsylvania
Immigrant Legal Resource Center
Immigration Advocates Network
Immigration Center for Women and Children
International Refugee Assistance Project (IRAP)
International Rescue Committee
Knight First Amendment Institute at Columbia University
Korean Community Center of the East Bay
Massachusetts Immigrant and Refugee Advocacy Coalition
MediaJustice
Muslim Advocates
National Immigration Law Center
OneAmerica
PEN America
Pro Bono Net
Seattle Office of Immigrant and Refugee Affairs (OIRA)
Service Employees International Union (SEIU)
South Asian Americans Leading Together (SAALT)
South Asian Network
Tamizdat
UnidosUS
West African Community Council