CENTER FOR DEMOCRACY & TECHNOLOGY

Department of State Desk Officer
Office of Information and Regulatory Affairs
Office of Management and Budget
725 17th Street, N.W.
Washington, DC 20503

September 27, 2018

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. 1405-0185

Dear Office of Management and Budget:

The Center for Democracy & Technology (CDT) appreciates the opportunity to comment on the Department of State's (DOS) proposals to expand information collected from 14.7 million immigrant and nonimmigrant visa applicants to include: social media identifiers used during the past five years; as well as telephone numbers and email addresses used in the past five years, and international travel over the past five years.[1] CDT has consistently opposed DOS's past social media collection proposals for many reasons including the fact that such collection would chill free speech and association and inhibit the right to anonymity, in return for little security benefit.[2] Indeed, we raised these concerns with DOS with respect to this proposed collection back in May.[3] Our comment in full to DOS is included as an attachment to this letter. Thus far, DOS has not been responsive to these criticisms, including concerns that they substantially underestimate the expense of such a program. Social media identifiers will yield messy and multidimensional data sets, from which meaning will be difficult if not impossible

[1] U.S. Dep't of State, 30-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa (Federal Register Number 2018-18594), Federal Register (Aug. 28, 2018), https://www.federalregister.gov/documents/2018/08/28/2018-18594/30-day-notice-of-proposed-information-collection-application-for-nonimmigrant-visa; U.S. Dep't of State, 30-Day Notice of Proposed Information Collection: Electronic Application for Immigrant Visa and Alien Registration (Federal Register Number 2018-18595), Federal Register (Aug. 28, 2018), https://www.federalregister.gov/documents/2018/08/28/2018-18595/30-day-notice-of-proposed-information-collection-electronic-application-for-immigrant-visa-and-alien.

[2] Center for Democracy & Technology, 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 (May 29, 2018), https://cdt.org/files/2018/05/CDT-Comment-State-Department-Information-Collection.pdf; Brennan Center, Re: 82 Fed. Reg. 6180, OMB Control No. 1405-0226; Supplemental Questions for Visa Applicants (Oct. 2, 2017), https://www.brennancenter.org/sites/default/files/StateDeptcomments-10.2.2017.pdf; Brennan Center, 82 Red. Reg. 20956, OMB Control No. 2017-08975; Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants (May 18, 2017), https://www.brennancenter.org/sites/default/files/analysis/State%20Dept%20Information%20Collection%20Comments%20-%2051817_3.pdf.

[3] Center for Democracy & Technology, 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 (May 29, 2018), https://cdt.org/files/2018/05/CDT-Comment-State-Department-Information-Collection.pdf.

to parse. Given that the average internet user has seven social media profiles,[4] this proposal would introduce significant noise and little if any discernable signal to the visa screening process. We urge the Office of Management and Budget (OMB), in its oversight role, to fully consider these concerns.

We specifically wish to highlight two issues which we discuss in greater detail in the attached comment:

1) Social media screening is unlikely to yield relevant security information.
    - Research demonstrates that expressive conduct like social media activity is not a valid predictor of one's propensity to commit an act of violence.[5]
    - DOS has not demonstrated that social media data will provide it with the ability to better enforce the Immigration and Nationality Act, or that its vetting would be hampered without this data.
    - There is no evidence to suggest that DOS has developed a strategy for evaluating social media data.
    - Social media screening is comically easy for bad actors to circumvent.

2) Social media content is not easily interpreted and will likely lead to the use of problematic algorithmic screening.
    - Social media communications are idiosyncratic and not easily decipherable, particularly those that employ slang, sarcasm, or non-textual information like emojis, GIFs and "likes." Undoubtedly visa applicants will also use foreign languages.
    - DOS is requesting more data than human analysts could possibly review.
    - In order to analyze the data collected, DOS may turn to automated tools to assess social media data. However, these tools are would be inherently technologically deficient and prone to discrimination. As CDT has explained in a recent white paper,[6] automated tools for analyzing the text of social media posts cannot reliably interpret the meaning of a post or the speaker's intent.

We urge OMB to withhold its approval of this proposed information collection because DOS's proposal will fail to achieve its stated purpose of aiding the evaluation of an applicant's eligibility for a visa. Instead this costly collection will discourage individuals from applying to enter the United States, will

[4] Jason Mander, *Internet Users Have Average of 7 Social Accounts*, GLOBALWEBINDEX (June 9, 2016), https://blog.globalwebindex.com/chart-of-the-day/internet-users-have-average-of-7-social-accounts/.
[5] Patel, Faiza & Koushik, Meghan, Countering Violent Extremism, Brennan Center for Justice (2017) p. 15 https://www.brennancenter.org/sites/default/files/publications/Brennan%20Center%20CVE%20Report_0.pdf ("Extreme or radical views are often assumed to lie at the heart of terrorism. But evidence shows that the overwhelming majority of people who hold radical beliefs do not engage in, nor support, violence.")
[6] Natasha Duarte, Emma Llanso & Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis*, Center for Democracy & Technology (Nov. 2017), https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf.

induce nominal mistakes in applications that could be cause for visa denial or revocation, and will chill freedom of speech, association and inhibit the right to privacy.

Respectfully submitted,

Emma Llansó
Mana Azarmi

Center for Democracy & Technology

CENTER FOR DEMOCRACY & TECHNOLOGY

Bureau of Consular Affairs, Visa Office
U.S. Department of State
2201 C Street, N.W.
Washington, DC 20520

Department of State Desk Officer
Office of Information and Regulatory Affairs
Office of Management and Budget
725 17th Street, N.W.
Washington, DC 20503

May 29, 2018

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

Introduction

CDT urges the State Department (DOS) to withdraw the agency's proposed information collection under Public Notices 10260 and 10261. Published March 30, 2018, DOS proposes to ask all immigrant and nonimmigrant visa applicants to provide social media identifiers, and email addresses used in the past five years, among other information. This astronomical collection would have an immediate impact on 14.7 million visa applicants, and thousands, if not millions, more third parties whose data could be collaterally reviewed.[1]

DOS's proposal lacks sufficient guidance for visa applicants, consequently chilling the applications of the travelers and immigrants the United States seeks to attract. The data returned from this bulk demand for data may be used to facilitate data mining or encourage the government to pursue unreliable algorithmic screening processes. Social media screening is an unproven security tactic that will invite abuse in exchange for little benefit, and the screening of social media data will chill visa applicants' and U.S. persons' freedom of expression and, association, and will inhibit visa applicants' right to anonymity. It is vital that DOS abandon this effort.

I. The State Department's Notice is Vague and Overbroad and Will Lead to Unintentionally Incomplete Applications and Adverse Determinations

DOS's proposal to demand social media identifiers used in the last five years is overbroad and fails to provide visa applicants with sufficient guidance. This will needlessly cause visa applicants to commit

[1] *See* U.S. Dep't of State, Notice for Request for Public Comment on Agency Information Collection Activities; Proposals, Submissions, and Approvals: Application for Nonimmigrant Visa (Federal Register Number 2018-06496), Regulations.gov (Mar. 30, 2018), https://www.regulations.gov/document?D=DOS-2018-0002-0001.

nominal errors in their applications, ultimately leaving them vulnerable to arbitrary denial of a visa or potential future denial or revocation of an immigration benefit.

DOS first began requiring visa applicants to provide their social media identifiers in May 2017, via emergency Public Notice 10065.[2] DOS requested "[s]ocial media platforms and identifiers, also known as handles, used during the last five years" from only a subset of visa applicants. This emergency notice became permanent in October 2017.[3] CDT and other civil liberties organizations opposed this collection for many reasons.[4] Significantly, DOS failed to define 'social media platforms,' which made the notice fatally ambiguous, as applicants could only guess what DOS meant by "social media platform."[5]

DOS has now proposed to expand this collection to all nonimmigrant and immigrant visa applicants, almost 15 million people in total.[6] In response to our early criticism, DOS specified a non-exhaustive list of 20 social media platforms from which it seeks to collect social media identifiers. This proposal requires applicants to provide their social media for any of the following platforms if used in the last five years: ask.fm, Douban, Facebook, Flickr, Google+, Instagram, Linkedin, MySpace, Pinterest, Qzone, Reddit, Sina Weibo, Tencent Weibo, Tumblr, Twitter, Twoo, Vine, Vkontakte, Youku, Youtube.[7] DOS is also again including an open-ended solicitation for any other social media platforms and handles applicants can voluntarily disclose.

Despite these clarifications, this proposed request is still vague and overbroad. Neither the notice nor any of the supporting documents has properly addressed the consequences of an applicant mistakenly failing to include a social media handle. The requirement to report all social media handles for these 20 platforms scopes too broadly: It is not reasonable to expect a visa applicant to remember all of the social media platforms they have used in the last five years. A report in 2017 found that the average person has 7.6 active social media accounts, with the number rising to 8.7 for those aged 16-34.[8] Visa applicants may temporarily create an account and try a new social media platform before deciding

---

[2] *See* U.S. Dep't of State, Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants, FederalRegister.gov (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.

[3] *See id.*

[4] *See* Brennan Center, Re: 82 Fed. Reg. 6180, OMB Control No. 1405-0226; Supplemental Questions for Visa Applicants (Oct. 2, 2017), https://www.brennancenter.org/sites/default/files/StateDeptcomments-10.2.2017.pdf.

[5] *See id.*

[6] *See* U.S. Dep't of State, *supra* note 1.

[7] DOS has promised to include an explanation for applicants instructing them that "they do not need to list accounts designated for multiple users within a business or other organization." Agency Information Collection Activities; Proposals, Submissions, and Approvals: Application for Nonimmigrant Visa, Supporting Documents, Regulations.gov (March 30, 2018), https://www.regulations.gov/document?D=DOS-2018-0002-0001.

[8] *See* Colm Hebblethwaite, *The average person has 7 social media accounts*, MARKETINGTECHNEWS (Nov. 17, 2017), https://www.marketingtechnews.net/news/2017/nov/17/average-person-has-7-social-media-accounts/.

whether or not to permanently add it to their internet rolodex. Unlike a primary email account, a social media account is often not permanently adopted, and platforms may not stay in business for long—longevity is the exception in social media services, not the rule. Indeed, while platforms may capture the attention of millions at one moment, the wrong update or design could send users running.[9] Platforms that fail to sufficiently monetize their service can also rise in prominence and crash shortly after. For example, Vine emerged in 2012 and shut down by 2016.[10] An applicant could have easily created an account on the service and long forgotten about it—but the DOS proposal could expect her to report that account until 2021.

Visa applicants can easily overlook or forget that they own certain accounts. As an example, when a person creates a Gmail account, Google automatically creates a YouTube account for that user;[11] this person may not realize that he has a YouTube account that he would need to report. Other platforms allow you to log in using your existing Facebook or Twitter account, or to create accounts using an existing email account. When it is frictionless by design to create a new profile or to sign up for a new service online, it is not likely that visa applicants will recall every profile or temporary login they have created in the past five years. It is unclear whether such relatively inactive accounts are subject to the mandatory disclosure requirement. It is also unclear under what circumstances applicants must disclose their "use" of these platforms. If an individual regularly reads or views posts on these platforms without creating an account, it is unclear what she should disclose on her application.

This proposal also fails to address the consequences applicants would suffer from failing to disclose every social media platform they use and their various identifiers. How will consular officials treat a mistaken failure to disclose? Is such an oversight sufficient grounds for denying a visa? Is such an mistake sufficient grounds for visa revocation if later discovered? If an applicant receives an immigrant visa and later becomes a citizen, would this be sufficient grounds for denaturalization? The parameters of the test must be made clear for applicants and immigration officials alike. Given the realities of how people adopt and discard social media accounts, and the high stakes for visa applicants, immigration officials should be presumptively lenient about such mistakes.

Moreover, applicants do not have guidance as to how their social media information will be assessed. DOS states that it will "collect this information for identity resolution and vetting purposes based on statutory visa eligibility standards."[12] While the notice's supporting documents include a provision stating that DOS will instruct its consular officials to not use the "collection of social media platforms and identifiers to deny visas based on applicants' race, religion, ethnicity, national origin, political

---

[9] *See* Kaya Yurieff & Seth Fiegerman, *Snapchat user growth stagnant amid redesign backlash*, CNN (May 1, 2018), http://money.cnn.com/2018/05/01/technology/snapchat-user-growth-redesign/index.html.

[10] *See* Catherine Rowell, *The rise and fall of Vine: A brief timeline*, BUSINESS CHIEF (Oct. 28, 2016), https://www.businesschief.com/technology/5614/The-rise-and-fall-of-Vine:-A-brief-timeline.

[11] *See* GOOGLE, https://support.google.com/youtube/answer/69961 (last visited May 29, 2018).

[12] *See* U.S. Dep't of State, *supra* note 1.

views, gender, or sexual orientation,"[13] there is little practical reason applicants should take comfort in this. There is no evidence that consular officials have been or will be trained to evaluate the data on social media platforms to assess an applicant's admissibility. Such failure to effectively design a social media screening program has plagued the U.S. government's social media initiatives since they were piloted. For example, in February 2017, the Office of the Inspector General (OIG) issued a report concluding that the Department of Homeland Security's (DHS) social media screening pilots do not have clear success criteria, and that DHS therefore may not be able to design an effective social media screening program.[14] The OIG also recommended that DHS develop and implement "well-defined, clear, and measurable objectives and standards"[15] to evaluate its social media screening pilot programs. These same recommendations would be highly applicable to any evaluation of social media information by DOS. But, with no apparent training of consular officials or public disclosure of plans to implement a training program or guidelines, visa applicants have ample cause to worry that DOS's program will be plagued by the same failures, which could lead to discrimination and mistaken negative interpretations of their social media data.

DOS has also not provided guidance on what it will do with the collected social media identifiers. This proposal fails to state whether social media screening will take place on a routine basis, or if profiles will be reviewed once an application has already been flagged. Applicants are also not told if information from their social media profiles will be collected, retained or shared with other agencies. Confusion still exists about the recent Systems of Record Notice issued from the Department of Homeland Security in October 2017.[16] There, DHS issued a notice stating that social media information would be retained in Alien Files, the official immigration files of immigrants and certain classes of nonimmigrants. It is unclear from that notice whether DOS intends to retain the social media identifiers and associated social media content in Alien Files. CDT and many other civil liberties organizations oppose the retention of social media data for many reasons, including the treatment of such individuals as second-class citizens.[17]

The consequences of the vagueness and overbreadth of this proposal are stark: the US will lose visa applicants from the very people the U.S. seeks to attract. Students will attend universities elsewhere and highly skilled employees will pursue opportunities in other countries.[18] A prohibitively difficult or

---

[13] *See id.* Supporting documents.

[14] *See* Office of Inspector General, Dep't of Homeland Security, DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success, No. OIG-17-40 (Feb. 27, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.

[15] *See id.* at 2.

[16] *See* Privacy Act of 1974; System of Records, Dep't of Homeland Security, FederalRegister.gov (Sept. 18, 2017), https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records.

[17] *See* Center for Democracy & Technology, *Coalition Letter Opposing DHS Social Media Retention*, CTR. FOR DEMOCRACY & TECH. (Oct. 19, 2017), https://cdt.org/insight/coalition-letter-opposing-dhs-social-media-retention/.

[18] *See* Richard Florida, *How Trump Threatens America's Talent Edge*, CITYLAB (Jan. 31, 2017) https://www.citylab.com/life/2017/01/how-trump-threatens-americas-talent-and-innovation-edge/515010/.

unattractive barrier to entry causes the U.S. to lose its competitive edge in education, business, and tourism. The U.S. will also lose out on cultural exchanges that have been vital to the growth of the country politically, socially, and commercially.

Visa adjudications are highly consequential: In the immigrant visa context, individuals seek long term entry into the United States in order to reunite with family members or to pursue employment opportunities. Nonimmigrants seek entry to study or travel and experience a new country. Consular officials have an incredible degree of discretion in making determinations as to who is eligible for admission into the United States.

Visa applicants are therefore vulnerable to bad data, mistaken negative inferences, the internalized prejudices of consular officials or ICE agents conducting security assessments. This proposal offers no recourse for redress. In many cases, applicants are not provided the reasoning for their visa denial or allowed to view the evidence that persuaded the consular official they were ineligible. Furthermore, due to the doctrine of consular non-reviewability, applicants are not afforded any path to appeal an adverse decision. Given this balance of power, it is vital that DOS focus on collecting, reviewing, and assessing reliable, digestible information that visa applicants can reasonably provide. Soliciting information that is difficult to remember in its entirety and— as discussed below—is also difficult to understand will only make the visa adjudications process slower, more discriminatory, and more arbitrary, and will chill individuals from seeking to enter the United States, to our detriment.

II. Social Media Content is Not Easily Interpreted and Will Likely Lead to the Use of Problematic Algorithmic Screening

DOS should not make visa determinations using context-dependent social media information. Social media communication, like most human interactions, is idiosyncratic. Deciphering the meaning of statements is difficult without an intimate understanding of the context in which they are made. Parsing meaning from text is particularly difficult when communications employ slang, sarcasm, or non-textual information including emojis, GIFs, and "likes." Visa applicants' social media content will also often contain foreign languages, further increasing the complexity of analyzing this information. Interpretive errors are thus not only likely but inevitable, and the relevance and value of social media is likely to be minimal.

Moreover, DOS is requesting more data than human analysts could possibly review. Given the realities of limited time and resources, coupled with the U.S. government's demonstrated appetite for big data analysis,[19] this collection raises concerns that data collected could be used to facilitate bulk data mining and algorithmic screening.

[19] *See, e.g.,* Immigration & Customs Enforcement Homeland Security Investigations (hereinafter "ICE-HSI"), "ICE-HSI Data Analysis Service: Solicitation Number HSCEMD-17-R-0010," FedBizOpps.Gov, June 12, 2017. *See* also Brennan Center for Justice, *ICE Extreme Vetting Initiative: A Resource Page*, https://www.brennancenter.org/analysis/ice-extreme-vetting-initiativeresource-page.

Recently, Immigration and Customs Enforcement (ICE) explored establishing an automated vetting system that would input applicants' social media data into predictive machine-learning models to generate investigative leads . This proposal, known as "Visa Lifecycle Vetting" (formerly "Extreme Vetting"), originated from President Donald Trump's immigration directives,[20] including Executive Order 13780, known as "the Muslim Ban."[21] While ICE has halted the machine-learning aspect of this initiative due to cost and logistical constraints, ICE has yet to acknowledge some of the inherent deficiencies with machine-based vetting or confirm that it will not continue to pursue the creation of an automated screening program.[22] Specifically, ICE sought to "evaluate an applicant's probability of becoming a positively contributing member of society as well as their ability to contribute to national interests,"[23] and predict whether those entering the U.S. intended to commit a crime or terrorist attack once they arrived here. Currently ICE has not described precisely how this program's replacement would work, other than saying that it will for now solicit a "labor contract" for manual—or human review—monitoring of social media.[24]

DOS's intent to access vast amounts of social media information, combined with its lack of a stated plan for using or parsing that information, raises the concern that DOS could attempt to implement an automated vetting system. Such a system would be inherently technologically deficient and prone to discrimination. As CDT has explained in a recent white paper,[25] automated tools for analyzing the text of social media posts cannot reliably interpret the meaning of a post or the speaker's intent. In the case of ICE's Visa Lifecycle Vetting plan, the criteria ICE sought to predict were amorphous and undefined, leading 54 of the nation's leading computer science experts sent a letter to DHS, stating that "no computational methods can provide reliable or objective assessments of the traits that ICE seeks to measure."[26] Because DOS has not indicated how it will use the social media data it collects, it is likely

---

[20] See ICE-HSI, "Extreme Vetting Initiative: STATEMENT OF OBJECTIVES (SOO)," June 12, 2017, FedBizOpps.Gov (hereinafter "Statement of Objectives").

[21] The White House Executive Order 13769, (Protecting the Nation from Foreign Terrorist Entry into the United States) (Mar. 6, 2017), https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states-2/.

[22] *See* Drew Harwell & Nick Miroff, *ICE just abandoned its dream of 'extreme vetting" software that could predict whether a foreign visitor would become a terrorist*, WASH. POST (May 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/.

[23] *See id.*

[24] Jake Laperruque, *ICE Backs Down on "Extreme Vetting" Automated Social Media Scanning*, PROJECT ON GOVERNMENT OVERSIGHT (POGO) (May 23, 2018), http://www.pogo.org/blog/2018/05/ice-backs-down-on-extreme-vetting-automated-social-media-scanning.html; *see also*, Natasha Duarte, *ICE Finds Out It Can't Automate Immigration Vetting. Now What?*, CTR. FOR DEMOCRACY & TECH. (May 22, 2018), https://cdt.org/blog/ice-cant-automate-immigration-vetting/.

[25] Natasha Duarte, Emma Llanso & Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis*, Center for Democracy & Technology (Nov. 2017), https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf.

[26] Center for Constitutional Rights, Coalition Letter to DHS Opposing Extreme Vetting Initiative (Nov. 16, 2017), https://ccrjustice.org/coalition-letter-dhs-opposing-extreme-vetting-initiative.

that any screening process that evaluates this social media data will involve the application of vague criteria, whether by algorithm or by human analyst. Because automated tools cannot conduct a nuanced evaluation of an applicant for entry into the United States, they would likely resort to proxies that are easier for computers to discern, such as the existence of religious imagery in photos. Such proxies would likely facilitate discriminatory targeting and would have very little actual power to predict eligibility.

The use of automated tools to predict whether a person, or a person's conduct, meets amorphous criteria would disproportionately harm minority groups. Machine learning models tend to reflect and even amplify any biases in the data used to train them. When these models are used for social media analysis, they often produce higher error rates when analyzing the speech of minority group members. For example, research shows that many popular social media analysis tools cannot accurately process tweets using language common among African-American Twitter users.[27] The tools in the study misidentified these tweets as not being in English at all, with one tool classifying the tweets as being in Danish with 99.9% confidence.[28] These biases are exacerbated by the fact that most available tools for performing this kind of analysis only work on English-language text.[29]

Indeed, one of the primary findings of our white paper was that "[d]ecisions based on automated social media content analysis risk further marginalizing and disproportionately censoring groups that already face discrimination,"[30] citing low accuracy rates for non-English languages and vernaculars associated with minority groups.

III. Social Media Screening Is Unlikely to Yield Relevant Security Information

There is no reason to believe that soliciting social media handles will yield a significant security benefit. DOS appears to believe that it can identify potential security threats by scrutinizing people's online speech, but research shows that such expressive conduct is not a valid predictor of one's propensity to commit an act of violence.[31] Furthermore, DOS has not demonstrated that social media data will

---

[27] Su Lin Blodgett & Brendan O'Connor, Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English at 1-2, Proceedings of the Fairness, Accountability, and Transparency in Machine Learning Conference (2017), https://arxiv.org/pdf/1707.00061.pdf.

[28] *Id.*

[29] *See* Julia Hirschberg & Christopher D. Manning, Advances in Natural Language Processing, 349 Science 261, 261 (July 17, 2015), https://cs224d.stanford.edu/papers/advances.pdf; Fredrik Johansson, Lisa Kaati & Magnus Sahlgren, Detecting Linguistic Markers of Violent Extremism in Online Environments, in Combating Violent Extremism and Radicalization in the Digital Era, 374–90 (2016), https://www.foi.se/download/18.3bca00611589ae7987820d/1480076542059/ FOI-S--5452--SE.pdf.

[30] *See* Duarte, Llanso & Loup, *supra* note 23, at 4, 8, 13.

[31] Patel, Faiza & Koushik, Meghan, Countering Violent Extremism, Brennan Center for Justice (2017) p. 15 https://www.brennancenter.org/sites/default/files/publications/Brennan%20Center%20CVE%20Report_0.pdf ("Extreme or radical views are often assumed to lie at the heart of terrorism. But evidence shows that the overwhelming majority of people who hold radical beliefs do not engage in, nor support, violence.")

provide it with the ability to better enforce the Immigration and Nationality Act. The supporting documents state that, "Department of State consular officers will use the information collected in the visa adjudication process, coordinating with other Department officials and with partner U.S. government agencies as appropriate, to determine applicants' eligibility for a visa under applicable U.S. law. *These determinations would not be possible without collecting this information.*"[32] However DOS provides no evidence to support this assertion. Indeed, DOS already has access to ample resources to assess an individual's admissibility for a visa.[33]

Additionally, there is no evidence to suggest that DOS has developed a strategy for evaluating social media data. As discussed above, a recent independent audit of DHS's social media pilot programs raised serious questions about their validity and efficacy.[34] The audit found that insufficient metrics were in place to measure the programs' effectiveness, and that absent valid metrics and evaluation criteria, the programs would be of little utility in planning or implementing additional social media screening initiatives. DOS has solicited social media data for a year, and no audit has been conducted to demonstrate the efficacy in that smaller collection. If the purpose of this initiative is greater security and enforcement of the INA, turning to social media data appears to occupy scarce resources while providing limited utility.

Furthermore, social media screening is comically easy for bad actors to circumvent. Knowing that DOS will be combing through social media data, would-be criminals and terrorists can simply delete or manipulate their online social media behaviors, and disclose only newly-created, sanitized social media accounts to DOS during the visa application process in order to evade detection. They may also simply use online services that do not appear on DOS's list. Thus, the kind of social media screening DOS is contemplating would be invasive, potentially abusive, and likely expensive, while yielding little actual security or screening benefit.

IV. This Proposal Will Chill Free Speech, Association, and Inhibit the Right to Anonymity

---

[32] Agency Information Collection Activities; Proposals, Submissions, and Approvals: Application for Nonimmigrant Visa, Supporting Documents, Regulations.gov (March 30, 2018), https://www.regulations.gov/document?D=DOS-2018-0002-0001 (emphasis added).

[33] One of their main sources is the Consular Consolidated Database. This database is "the repository of data flows between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), and other federal agencies that provide input into the visa and passport review and approval systems." U.S. Dep't of State, Privacy Impact Assessment (PIA) Consular Consolidated Database (CCD) Version 0.4.00.00 (July 17, 2015), https://www.state.gov/documents/organization/242316.pdf. Consular officials are aided in their screening efforts through the use of 'Security Advisory Opinions,' which is "a U.S. Government mechanism to coordinate third-agency checks on visa applicants about whom the State Department have security-related concerns." U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Visa Security Program Tracking System (Aug. 27, 2009), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_vsptsnet.pdf.

[34] *See* Office of Inspector General, Dep't of Homeland Security, DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success, No. OIG-17-40 (Feb. 27, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.

Demanding social media information will chill visa applicants' exercise of their rights to freedom of speech and association, as well as their right to anonymity. Applicants will feel pressure to self-censor, delete their social media accounts, and disengage from online spaces rather than risk denial of a visa, with negative consequences for their social, political, and business activities. For example, such individuals could feel pressure not to criticise a U.S. policy, or the policies of our allies. This is unacceptable and could curtail social and political movements around the world. In Iran, for example, use of social media has been credited with aiding activism for nearly a decade, from the Green Movement in 2009[35] to political demonstrations in January 2018.[36]

Applicants may also limit their social media engagements for fear that casual connections on social media may be perceived as a suspicious affiliation. For example, DOS could perceive an applicant's relationship with a Facebook friend or an Instagram follower as an intimate association, even though social media connections need not be based on any actual relationship. Current treatment of social media data in immigration provides cause for concern. Social media connections have already been used to allege gang affiliation in the United States, in both the criminal and immigration contexts.[37] ICE Homeland Security Investigations, a government agency that provides DOS with security screenings for suspect visa applicants, have alleged that a teenager's "friends" on Facebook is an indication of affiliation with gang members.[38] Photos in which young men wear popular sports team hats like the Chicago Bulls, LA Lakers, or popular music apparel are used to allege gang affiliation.[39] Such flimsy 'evidence' has been used to justify bond denials and denial of discretionary immigration benefits. And again, in the visa context applicants have no redress process or right to correct mistaken inferences.

---

[35] *See* Somayeh Moghanizadeh, Thesis: *The role of social media in Iran's Green Movement*, University of Gothenberg, May 2013, https://gupea.ub.gu.se/bitstream/2077/34206/1/gupea_2077_34206_1.pdf.

[36] *See* Samantha Madison, *How Social Media Has Changed the Way Political Movements Organize*, GOVERNMENTTECHNOLOGY.COM (Jan. 10, 2017), http://www.govtech.com/social/How-Social-Media-Has-Changed-the-Way-Political-Movements-Organize.html*; see also*, CBC News, *Social media plays 'extremely important' role in Iranian protests despite censorship*, CBC (Jan. 4, 2018), http://www.cbc.ca/news/technology/iran-protests-social-media-telegram-1.4471226; *see also* Sheera Frenkel, *Iranian Authorities Block Access to Social Media Tools*, N.Y. TIMES (Jan. 2, 2018), https://www.nytimes.com/2018/01/02/technology/iran-protests-social-media.html.

[37] Jareyah Bradley, New Report: Trends in Gang Allegations Against Immigrant Youth Analyzed by the ILRC, IMMIGRANT LEGAL RESOURCE CENTER (May 21, 2018), https://www.ilrc.org/new-report-trends-gang-allegations-against-immigrant-youth-analyzed-ilrc*; see also* Max Rivlin-Nadler, *How Philadelphia's Social Media-Driven Gang Policing Is Stealing Years From Young People*, THE APPEAL (Jan. 19, 2018), https://injusticetoday.com/how-philadelphias-social-media-driven-gang-policing-is-stealing-years-from-young-people-fa6a8dacead9.

[38] LAILA L. HLASS & RACHEL PRANDINI, IMMIGRANT LEGAL RESOURCE CENTER, DEPORTATION BY ANY MEANS NECESSARY: HOW IMMIGRATION OFFICIALS ARE LABELNG IMMIGRANT YOUTH AS GANG MEMBERS (2018) https://www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf.

[39] *Id.* at 11.

These stories are, unsurprisingly, becoming more common as social media screening is adopted by more agents of the U.S. government. As these scenarios proliferate, visa applicants will no doubt take steps to protect themselves, limiting their engagements on these platforms and restricting the individuals they connect with.

This proposal will not also chill the expressive activities of U.S. persons. Immigrant and nonimmigrant activists have long been responsible for important reforms in our society, and government social media monitoring will jeopardize their vital engagement in civic action. The public will lose valuable voices and perspectives in public debate if immigrants feel restrained in their freedom of speech. Furthermore, U.S. persons who are connected to visa applicants on social media may restrict their activity out of fear of collateral scrutiny by DOS. These U.S. persons may sanitize or delete their social media profiles. They may also limit their engagement with foreigners and visa applicants out of fear of surveillance, chilling the exercise of their free association rights, while stigmatizing and isolating immigrant communities.

Furthermore, this policy will chill the right to anonymous speech for applicants and U.S. persons, leading to negative repercussions on members of vulnerable communities, such as domestic violence victims and religious minorities. Due to legitimate privacy and security concerns, individuals often use anonymous social media profiles, alter their online profiles from their real-world identities, or list conflicting information across their social media handles. This is particularly true for domestic violence victims, who are often harassed and stalked online by their abusers, resulting in potentially deadly violence against victims and their families.[40] Furthermore, individuals from countries where disclosure of sensitive information would endanger their security and privacy, such as LGBTQ people, and religious, ideological and ethnic minorities, use anonymous online speech to seek assistance, advocate for their rights, and create community. Social media serves as an important outlet for these vulnerable populations. Fear that their online activities would be subjected to routine scrutiny and potential disclosure would chill the freedom of association and right to anonymous speech of both visa applicants and U.S. persons.

* * *

DOS's proposal will fail to achieve its stated purposes of aiding the evaluation an applicant's eligibility for a visa. Instead this collection will discourage individuals from applying to enter the United States, will induce nominal mistakes in applications that could be cause for visa denial or revocation, and will chill freedom of speech, association and inhibit the right to privacy. We urge DOS to withdraw this proposal.

---

[40] *See* Hadeel Al-Alosi, *Technology-facilitated abuse: the new breed of domestic violence*, THE CONVERSATION (Mar. 27, 2017), https://theconversation.com/technology-facilitated-abuse-the-new-breed-of-domestic-violence-74683; *see also* Matt Lindner, *Advocates work to keep victims of domestic violence safe on social media*, CHI. TRIB. (Dec. 29, 2016), http://www.chicagotribune.com/lifestyles/sc-domestic-violence-social-media-family-0103-20161228-story.html; *see also Domestic Violence and Privacy*, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), https://www.epic.org/privacy/dv/.

CENTER FOR DEMOCRACY & TECHNOLOGY

Respectfully submitted,

Emma Llansó
Natasha Duarte
Mana Azarmi
Alicia Loh

Center for Democracy & Technology