

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

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

May 29, 2018

RE: Application for Immigrant Visa and Alien Registration, OMB Control Number: 1405-0185, Docket Number: DOS-2018-0003, 83 Fed. Reg. 13806; Application for Nonimmigrant Visa, OMB Control Number: 1405-0182, Docket Number: DOS-2018-0002, 83 Fed. Reg. 13807

To Whom It May Concern:

We write once more to express our serious concern with expanding the Department of State’s (“the Department”) supplemental questionnaire to all 14,710,000 visa applicants. Such an expansion will negatively impact free speech and association rights, potentially endanger vulnerable visa applicants, and undermine the right to freely exercise one’s religion without discrimination.

Muslim Advocates, a civil rights organization dedicated to ensuring freedom and justice for Americans of all faiths, has commented numerous times on the State Department’s recent attempts to make the visa application process evermore burdensome and invasive, and through this comment we again urge the Office of Management and Budget (“OMB”) to reject the Department’s requests.¹ In our earlier comments—submitted both when OMB first considered the Department’s request on an “emergency” basis and again when it considered making that request permanent—we expressed our deep concerns that the questionnaire imposes an intrusive and discriminatory burden on the Muslim community without providing a national security benefit. The Department’s latest iteration, a significant expansion of the original measure, has only intensified those concerns. Further, we have not received any additional information explaining the nature of the emergency and associated policies and procedures, despite making such requests nearly a year ago pursuant to the Freedom of Information Act.²

¹ See Letter to OMB and U.S. Department of State from Muslim Advocates, Re: Supplemental Questions for Visa Applicants, OMB Control Number: New, DS-5535, Docket Number: DOS-2017-0019 (May 18, 2017), Letter to OMB and U.S. Department of State from Muslim Advocates, RE: Supplemental Questions for Visa Applicants, OMB Control Number: 1405-0226, DS-5535, Docket Number: DOS-2017-0032 (Oct. 2, 2017), Letter to OMB and U.S. Department of State from Muslim Advocates, Re: Supplemental Questions for Visa Applicants, OMB Control Number: 1405-0226, DS-5535 (Dec. 20, 2017).

² See Letter to U.S. Department of State from Muslim Advocates, Americans United for Separation of Church and State, the Southern Poverty Law Center, the Brennan Center for Justice, and Professor Shoba

I. Introduction

The most recent OMB Notices of Proposed Information Collection (“Notices”)—one addressing immigrants¹ and the other non-immigrants²—will dramatically increase the Department’s collection of information from visa applicants. These Notices will not only uniquely impact Muslims and applicants from Muslim-majority countries, but also magnify the current information collection program’s harms: the infringement on individuals’ freedoms of speech and association as well as the unjustified expenditure of federal resources.

OMB initially approved the Department’s original request to collect supplemental information on May 23, 2017 only as a temporary “emergency” measure. The proposed supplemental questionnaire asked applicants to provide: (1) travel history during the last fifteen years, including source of funding for travel; (2) address history during the last fifteen years; (3) employment history during the last fifteen years; (4) all passport numbers held by the applicant and countries of issuance; (5) names and dates of birth for all siblings; (6) names and dates of birth for all children; (7) names and dates of birth for all current and former spouses, or civil or domestic partners; (8) social media platforms and identifiers, also known as handles, used during the last five years; and (9) phone numbers and email addresses used during the last five years.³

The original request only applied to an undefined “subset” of applicants—an estimated 65,000 respondents—that the Department argued “warrant[ed] increased scrutiny.”⁴ This initial request neither offered guidance on how to identify those particular applicants nor justified its estimated figure. However, as we have noted before, the estimate correlated with the number of non-immigrant visas issued to citizens from the six countries listed in the President’s revised March 6, 2017 travel order.⁵

Sivaprasad Wadhia, Re: Freedom of Information Act Requesting Regarding Visa Applicant Vetting Policies and Procedures (July 20, 2017).

¹ 60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration, 83 Fed. Reg. 13,806 (Mar. 30, 2018).

² 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, 83 Fed. Reg. 13,807 (Mar. 30, 2018).

³ Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 20,956 (May 4, 2017).

⁴ *Id.*

⁵ Exec. Order No. 13,780, 82 Fed. Reg. 13,209 (Mar. 6, 2017); *see also* Letter to OMB and U.S. Department of State from Muslim Advocates, RE: Supplemental Questions for Visa Applicants, OMB Control Number: 1405-0226, DS-5535, Docket Number: DOS-2017-0032 (Oct. 2, 2017).

Then, on August 3, 2017, the Department published a second request that proposed making the emergency measure permanent for this “subset.”¹ Having never justified the use of the emergency procedure in the first place, the Department again failed to explain its reasons for permanently embedding the questionnaire in the visa application process. The Department continued to set its “best estimate” of affected visa applicants at 65,000, again without any stated justification.

Now, the Department hopes to expand its unjustified data collection program to 14,710,000 people—nearly all visa applicants, immigrant and non-immigrant. Though widening the net obscures the underlying targeting of Muslims and people from Muslim-majority countries, President Trump has made the purpose of these Notices clear. In addition to asserting that “Islam hates us”² and repeating the disproven story that Muslims in New Jersey cheered during the September 11 attacks,³ he made campaign promises to create a “Muslim ban” and “Muslim registry.”⁴ Both promises will be further on their way to enactment (albeit unofficially) with the approval of the State Department’s latest Notices.

The White House’s positions have normalized prejudiced views, and the Department’s “extreme vetting” Notices will enshrine them in the visa application system. Moreover, the Notices will have a chilling effect on applicants’ speech and relationships on social media platforms, not only due to applicants’ fears of misunderstandings by immigration officials, but also out of fear that this information could be disclosed—intentionally or not—to other parties. Some applicants, such as political dissidents or members of the LGBT community, could face terrible consequences if their social media profiles are shared with foreign governments.

The cost of these measures therefore far outweighs any benefits that could come from the Department’s request. The Notices infringe on religious liberty, freedom of speech, and freedom of association, yet yield little to no national security benefit. Beyond the costs to individual rights, government officials will spend an estimated 22,834,167 additional hours—equivalent to over 2,600 years—collecting and examining the data annually. The Notices will likely involve exorbitant expenses as well, but despite inviting comments to “[e]valuate the accuracy of our

¹ 60-Day Notice of Proposed Information Collection: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 36,180 (Aug. 3, 2017).

² Theodore Schleifer, *Donald Trump: ‘I think Islam hates us’*, CNN, Mar. 10, 2016, <http://www.cnn.com/2016/03/09/politics/donald-trump-islam-hates-us/>.

³ Lauren Carroll, *Fact-checking Trump’s Claim that Thousands in New Jersey Cheered When World Trade Center Tumbled*, POLITIFACT, Nov. 22, 2015, <http://www.politifact.com/truth-o-meter/statements/2015/nov/22/donald-trump/fact-checking-trumps-claim-thousands-new-jersey-ch/>; see also Tessa Berenson, *Video Debunks Trump’s Claim That Thousands of American Muslims Celebrated 9/11*, TIME, Dec. 1, 2015, <http://time.com/4131439/donald-trump-muslims-9-11-video/>.

⁴ See Abby Phillip & Abigail Hauslohner, *Trump on the Future of Proposed Muslim Ban, Register: ‘You Know My Plans’*, WASH. POST, Dec. 22, 2016, <https://www.washingtonpost.com/news/postpolitics/wp/2016/12/21/trump-on-the-future-of-proposed-muslim-ban-registry-you-know-my-plans/>; see also Mica Rosenberg & Julia Edwards Ainsley, *Immigration Hardliner Says Trump Team Preparing Plans for Wall, Mulling Muslim Registry*, REUTERS, Nov. 15, 2016, <http://www.reuters.com/article/us-usa-trump-immigration-idUSKBN13B05C>.

estimate of the time and cost burden for this proposed collection,” they do not account for the financial cost.¹

For these and the reasons discussed below, we strongly urge OMB to reject the Department’s Notices seeking to extend the supplemental questionnaire to all visa applicants.

II. The Proposed Information Collection Will Subject Visa Applicants to Severe Consequences.

A. Collecting Applicants’ Social Media Data Will Come at Significant Cost to Free Speech and Association.

Multiple studies show that people alter their behavior if they know (or fear) they are being watched.² Under the Department’s Notices, nearly 15 million visitors to the United States would be subject to the potential monitoring of their social media presences.³ Travelers will feel forced to either modify their social media use, perhaps deleting their accounts, or refrain from visiting the United States entirely.

1. Given the High Stakes Involved and the Likelihood of Misinterpretation, Providing Social Media Handles to Enter the Country Will Unavoidably Chill Valuable Speech.

The Notices will cause visa applicants to refrain from any social media activity that could possibly alarm American border agents or cause embarrassment on the travelers’ part – attending certain events, taking certain pictures, posting certain articles or comments, or communicating with certain individuals. This is especially true given that the Notices do not

¹ 60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration, 83 Fed. Reg. 13,806 (Mar. 30, 2018); *see also* 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, 83 Fed. Reg. 13,807 (Mar. 30, 2018).

² *See, e.g.,* Jon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L. J. 1, 117 (2016) (finding a statistically significant decrease in traffic to Wikipedia articles on topics that raise privacy concerns following Edward Snowden’s NSA/PRISM online surveillance revelations); Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA, May 13, 2016 (finding Americans’ concerns with online privacy and security have led them to limit their online activity), <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>; Elizabeth Stoycheff, *Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM’N QUARTERLY 296 (2016) (finding people self-censor when told they are being monitored by the NSA, expressing opinions if they feel they are in the majority and suppressing them if not), <http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255>.

³ *See* Rachel Levinson-Waldman, *Why the Government Should Abandon Its Plan to Vet Foreigners on Facebook*, WASH. POST, Dec. 4, 2017, <https://www.washingtonpost.com/news/posteverything/wp/2017/12/04/why-the-government-should-abandon-its-plan-to-vet-foreigners-on-facebook/> (“[A]s a practical matter, it is highly implausible that a program purporting to scrutinize the Internet would pick up only materials that are posted by or related to foreign visitors; rather, it will sweep in vast quantities of content about lawful permanent residents and citizens as well.”).

specify what types of information could raise suspicion, and the Department has not released any guidance on what factors agents will consider on this front. Travelers are already becoming more vigilant in self-policing due to concerns about being denied entry into the United States. In fact, ABTA, a U.K. trade association of travel companies, warned those vacationing in the U.S. to watch what they say on social media after two British tourists' jokes on Twitter were misinterpreted, resulting in the pair being denied entry and detained overnight.¹

This chilling effect will be particularly strong among Muslim travelers and those from Muslim-majority countries. Due to cultural and language differences, those travelers' online postings will invite increased scrutiny from border officials, even if (this time) Muslims are not being exclusively targeted by the Department's Notices. Border agents may take one look at an individual's social media profile and, based on an article the applicant posted about Islamic teachings or a photo of her wearing a hijab, instantly assume that person is dangerous.

Already, misunderstandings and biases hinder travel for Muslims and persons assumed to be Muslim. For example, in January 2017, a 5-year-old boy, a U.S. citizen whose mother is Iranian, was handcuffed and detained for four hours.² A month later, Muhammad Ali's son was allegedly detained with his mother at a Florida airport and questioned about his religion for over an hour.³ In July 2017, the entire Afghan girls' robotics team was set to travel to the United States to participate in a science competition only to have their visas initially denied.⁴

Even beyond formal government actions, the fears and increased scrutiny of fellow passengers subject certain travelers to unwarranted treatment. In November 2015, an American Muslim who runs a pizzeria in Philadelphia and his friend were pulled aside during an airline boarding process because a fellow passenger heard them speaking Arabic.⁵ That same day, six Muslim passengers were removed from a plane after asking to sit together.⁶ In March 2016, a

¹ *Caution on Twitter Urged as Tourists Barred from US*, BBC NEWS, March 8, 2012, <http://www.bbc.com/news/technology-16810312>.

² Rachel Roberts, *White House Claims Five-year-old Boy Detained in US Airport for Hours 'Could Have Posed a Security Threat'*, INDEPENDENT, Jan. 31, 2017, <https://www.independent.co.uk/news/world/americas/white-house-five-year-old-boy-detained-dulles-international-airport-hours-sean-spicer-pose-security-a7554521.html>.

³ Don Melvin & Molly Roecker, *Muhammad Ali Jr. Detained at Airport, Asked About Being Muslim: Lawyer*, NBC NEWS, Feb. 25, 2017, <https://www.nbcnews.com/news/us-news/muhammad-ali-jr-detained-airport-asked-about-being-muslim-lawyer-n725571>.

⁴ Laurel Wamsley, *Afghan Girls Robotics Team Allowed to Enter U.S. For Competition*, NPR NEWS, Jul. 13, 2017, <http://www.npr.org/sections/thetwo-way/2017/07/13/537050073/afghan-girls-robotics-team-allowed-to-enter-u-s-for-competition>.

⁵ Karen Araiza, *Philly Pizza Shop Owner Calls 911 After He Says He Was Profiled on Flight Home*, WCAU NBC 10, Nov. 15, 2015, <http://www.nbcphiladelphia.com/news/local/Philly-Pizza-Shop-Owner-Profiled-Southwest-Airlines-351944441.html>.

⁶ Michelle Gallardo & Stacey Baca, *Flight from Midway to Houston Delayed, Passengers Removed*, ABC7 EYEWITNESS NEWS, Nov. 18, 2015, <http://abc7chicago.com/news/flight-from-midway-to-houston-delayed-passengersremoved/1090031/>.

University of California, Berkeley student was removed from a flight after he called his uncle and spoke to him in Arabic about attending a speech by United Nations Secretary General Ban Ki-moon.¹ Two months later, a passenger with “dark, curly hair, olive skin and an exotic foreign accent” was removed from a plane after a passenger thought the math problem he was working on looked suspicious.² Passengers are not the only ones who are at risk: in January 2017, a man with a layover at JFK airport kicked and berated a Delta employee, shouting, “(Expletive) Islam. (Expletive) ISIS. Trump is here now. He’s going to take care of all of you.”³ These instances represent only a fraction of those reported.⁴

These actions by fellow travelers are unsurprising given the rise in prejudice against Muslims and popular misconceptions about their faith. One public opinion poll found sixty-one percent of Americans view Islam negatively and forty-four percent express unfavorable views of Muslims.⁵ In addition, hate crimes against Muslims are on the rise—between 2014⁶ and 2015,⁷ attacks spiked by sixty-seven percent, reaching the highest number of incidents since 2001. In 2016, that figure rose another nineteen percent.⁸

But while religious biases already play an active role in inhibiting Muslims’ travel, the questionnaire would entrench them in the visa application process without the appropriate safeguards to protect against unlawful discrimination. Muslims—or those from Muslim

¹ Liam Stack, *College Student Is Removed From Flight After Speaking Arabic on Plane*, N.Y. TIMES, Apr. 17, 2016, <https://www.nytimes.com/2016/04/17/us/student-speaking-arabic-removed-southwest-airlines-plane.html>.

² Catherine Rampell, *Ivy League Economist Ethnically Profiled, Interrogated for Doing Math on American Airlines Flight*, WASH. POST, May 7, 2016, https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doing-math-on-american-airlines-flight/?utm_term=.b4b3a850d923.

³ Sean Rossman, *DA: Man Kicked Muslim Woman at JFK Airport, Said ‘Trump is Here Now’*, USA TODAY, Jan. 27, 2017, <https://www.usatoday.com/story/news/nation-now/2017/01/27/da-man-kicked-muslim-woman-jfk-airport-said-trump-here-now/97145286/>.

⁴ Letter from Muslim Advocates and the Legal Defense Fund to Kathryn Thomson, General Counsel, U.S. Department of Transportation, May 11, 2016, https://www.muslimadvocates.org/wp-content/uploads/Final-Letter-to-DOT-051116_MA-NAACP-LDF.pdf.

⁵ Shibley Telhami, *What Americans Really Think About Muslims and Islam*, BROOKINGS INST., Dec. 9, 2015, <https://www.brookings.edu/blog/markaz/2015/12/09/what-americans-really-think-about-muslims-and-islam/>.

⁶ Incidents, Offenses, Victims, and Known Offenders by Bias Motivation, 2014 Hate Crime Statistics, FED. BUREAU OF INVESTIGATION, <https://ucr.fbi.gov/hate-crime/2014/tables/table-1>.

⁷ Incidents, Offenses, Victims, and Known Offenders by Bias Motivation, 2015 Hate Crime Statistics, FED. BUREAU OF INVESTIGATION, <https://ucr.fbi.gov/hate-crime/2015/tables-and-data-declarations/itabledatadecpdf>.

⁸ Incidents, Offenses, Victims, and Known Offenders by Bias Motivation, 2016 Hate Crime Statistics, FED. BUREAU OF INVESTIGATION, <https://ucr.fbi.gov/hate-crime/2016/tables/table-1>.

majority countries—would face unique risks of their social media presences being misconstrued. Despite this risk, the Department’s Notices do not mention any plan to hire linguistic or cultural experts to contextualize and evaluate individuals’ profiles. After all, doing so would be tremendously expensive. Instead, decisions about which profiles warrant additional scrutiny will likely be left to the subjective, gut-instinct-based will of border officials ill-equipped to adequately and fairly make such decisions. Unintentional or intentional biases will become an ingrained part of the selection criteria. In a nation founded in part on the freedom to practice religion without government interference, crucial determinations as to who may enter the country should not be rooted in cultural or social biases removed from any legitimate national security interest.

2. The Proposed Collection Will Adversely Impact Individuals’ Association Rights, as Social Media Users May Hesitate to Communicate or Be Otherwise Connected to an Individual Who May Be Seen as a Threat.

Examining applicants’ relationships on social media presents a unique threat to freedom of association. Despite the fact that many online “friends” are not significant real-life connections,¹ “following” or “friending” a foreign- or suspicious-looking individual on a social media site could have severe consequences should the Department’s Notices take effect, such as preventing entry into the United States. Applicants may, as a result, avoid all relationships, however tangential, that border agents could possibly misconstrue.

The same concerns of disparate impacts on Muslims and Arabic speakers discussed in the previous section apply here, as well. As a result of underlying biases, agents may be more suspicious of individuals with friends from certain regions or countries, and subject such individuals’ applications to greater scrutiny. The Notices could then yield disproportionate self-censorship, requiring people with ties to those areas to be especially cautious and restrictive of their online associations.

Moreover, the Notices could disadvantage journalists, scholars, or human rights workers with social media connections that may raise suspicion. For example, one Pulitzer Prize-nominated journalist who reports on extremist groups connects with sources through Twitter, Instagram, Tumblr, and Telegram.² An agent looking at her social media presence out of context might misunderstand the nature of such online relationships. The critical investigative reporting these journalists are doing could be used against them in applying for a visa, which may make reporters feel forced to cut off certain relationships and severely limit their—and by extension, the public’s—access to information.

¹ Nicole B. Ellison, Charles Steinfield & Cliff Lampe, *Connection Strategies: Social Capital Implications of Facebook-enabled Communication Practices*, 13 *NEW MEDIA & SOCIETY* 873, Jan. 2011 (finding survey respondents had a median of 300 Facebook “friends” but reported only an average of 75 were “actual” friends), <https://doi.org/10.1177/1461444810385389>.

² Caitlin Roper, *How One Journalist Uses Social Media to Get Inside the Minds of ISIS*, *WIRED*, Aug. 3, 2016, <https://www.wired.com/2016/08/rukmini-callimachi-new-york-times-isis/>.

B. Collecting Social Media Identifiers Could be Exceptionally Dangerous When that Information is Intentionally or Inadvertently Shared with Other Agencies and Governments.

1. The State Department Will Likely Share this Information with the Department of Homeland Security, Which is Developing an Ill-Advised, Automated “Extreme Vetting Initiative.”

Given the Notices’ rapid escalation in scope and the Department’s limited resources, the Department will likely share the collected questionnaire data with the Department of Homeland Security (“DHS”). This is extremely problematic, not only because DHS’s mission and uses of the data may differ from the Department’s, but also because DHS will likely employ automated systems involving bulk data mining and algorithmic analysis. These systems are woefully ineffective at their stated goal, which is to evaluate human communication.¹ In fact, DHS’s Extreme Vetting Initiative has faced considerable criticism, including in a letter from 54 experts at Google, MIT, Microsoft, and elsewhere who assert, “no computational methods can provide reliable or objective assessments of the traits that ICE seeks to measure.”²

These tools will inevitably lead to infringement on individuals’ privacy and prejudicial decision-making. According to the Center for Democracy & Technology, studies show that natural language processing tools reflect and even amplify social bias embedded in the text from which they learn.³ In other words, artificial intelligence is not magic; it’s math—and biased inputs yield biased outputs. For example, researchers at MIT and Microsoft found that facial recognition systems had far higher error rates with female faces than male, and with darker-skinned faces than lighter-skinned.⁴ As another example, studies show disparate law enforcement practices may render algorithms that rely on biased data prone to targeting marginalized groups.⁵

¹ Ahmed Abbasi, Ammar Hassan, & Milan Dhar, *Benchmarking Twitter Sentiment Analysis Tools*, in Proceedings of the 9th Conference on Language Resources and Evaluation, Reykjavik, Iceland (2014), <https://pdfs.semanticscholar.org/doi/10.1145/2518800.2518801>.

² Letter from Hal Abelson, ET AL., to Elaine C. Duke, Acting Secretary of Homeland Security, Nov. 16, 2017 (“In all likelihood, the proposed system would be inaccurate and biased.”), <https://www.brennancenter.org/sites/default/files/Technology%20Experts%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%202011.15.17.pdf>.

³ Natasha Duarte, *Mixed Messages: The Limits of Automated Social Media Content Analysis*, CTR. FOR DEMOCRACY & TECH., Nov. 2017, at 4, <https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf>.

⁴ Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACH. LEARNING RESEARCH 1 (2018), <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

⁵ See, e.g., Julia Angwin, ET AL, *Machine Bias*, PROPUBLICA, May 23, 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>, Julia Angwin and Jeff Larson, *Bias in Criminal Risk Scores is Mathematically Inevitable, Researchers Say*, PROPUBLICA, Dec. 30, 2016, <https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say>.

Automated systems may also have “disparate accuracy levels for minority populations” that may use dialects or different language patterns.¹ One University of Massachusetts-Amherst study found a popular algorithm identified tweets written in African-American vernacular English as Danish with more than ninety-nine percent confidence.² For non-English speakers, the risks are even higher, as most tools available today are effective only for English text and will likely misinterpret other languages. For example, last year a Palestinian man was held for questioning by Israeli police after a machine incorrectly translated his Facebook post (which said “good morning” in Arabic) to “attack them” in Hebrew.³

Even if the information is not shared with DHS, the Department might develop its own parallel automated processes. In the Notices, the Department indicates it is seeking comments on “the use of automated collection techniques or other forms of information technology” in order to reduce the reporting burden. Given its disparate impacts and inaccurate results, automated technology should not be used by either department to analyze individuals’ social media accounts. While efficiency and cost-effectiveness are important values, the border is not the place to implement this technology.

2. Programs in Which U.S. Intelligence Agencies Share Data With Foreign Governments May Put Visa Applicants in Danger if Their Social Media Profiles Reveal Behavior that is Innocuous in the U.S. but Criminal in Their Home Country.

Due to agreements under which U.S. intelligence agencies share data they collect—such as UKUSA⁴ and the Memorandum of Understanding with Israel⁵—the Department may be

¹ Duarte, *supra* note 33, at 4; *see also* Su Lin Blodgett & Brendan O’Connor, *Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English*, June 30, 2017 (“[C]urrent systems sometimes analyze the language of females and minorities more poorly than they do of whites and males.”), <https://arxiv.org/abs/1707.00061>.

² Su Lin Blodgett & Brendan O’Connor, *Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English*, 2017 Proceedings of the Fairness, Accountability & Transparency in Machine Learning Conference, <https://arxiv.org/pdf/1707.00061.pdf>.

³ Alex Hern, *Facebook Translates ‘Good Morning’ into ‘Attack Them’, Leading to Arrest*, THE GUARDIAN, Oct. 24, 2017, <https://www.theguardian.com/technology/2017/oct/24/facebook-palestine-israel-translates-good-morning-attack-them-arrest>.

⁴ UKUSA Agreement Release 1940-1956, National Security Agency, <https://www.nsa.gov/news-features/declassified-documents/ukusa/>; *see also* Janine McGruddy, *Multilateral Intelligence Collaboration and International Oversight*, 6 J. OF STRATEGIC STUDIES 214 (2013), <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1317&context=jss>, Scarlet Kim, ET AL., *Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements*, LAWFARE, April 23, 2018, <https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing>.

⁵ *NSA and Israeli intelligence: Memorandum of Understanding – full document*, THE GUARDIAN, Sep. 11, 2013, <https://www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document>; *see also* Matthew Brodsky, *What Makes US-Israeli Intelligence Co-operation ‘Exceptional’?*, THE GUARDIAN, Sep. 13, 2013, <https://www.theguardian.com/commentisfree/2013/sep/13/us-israeli-intelligence-cooperation-exceptional>.

bound to disclose the collected social media identifiers with other governments, putting visa applicants at risk in the process. For example, should a visa applicant's sexual orientation be shared with his or her home country, the applicant may be subjected to societal condemnation, harm, and even criminal penalties.¹ Disclosure could also endanger political activists or dissidents who use hidden profiles or alternate names to avoid persecution by their governments.² Similarly, journalists often use alternate profiles to contact sources while keeping their account names hidden for their safety.³ The consequences of disclosure for these individuals will compound the chilling effects of the infringements on free speech and association, similarly forcing visa applicants to either censor their social media activity or refrain from travelling to the United States altogether.

Even if the Department were not to share the questionnaire information at all, it could still be acquired if the appropriate cybersecurity protections are not in place. Unfortunately, both OMB⁴ and the Department⁵ have dealt with data breaches in recent years, highlighting the challenge of protecting information in the current climate of digital warfare. Collecting this information risks it being inadvertently exposed. The consequences that vulnerable groups could face if their data is disclosed are too serious to justify its collection and storage.

¹ *The State of LGBT Human Rights Worldwide*, AMNESTY INTERNATIONAL, <https://www.amnestyusa.org/the-state-of-lgbt-rights-worldwide/> (“Six countries (Mauritania, Sudan, Iran, Saudi Arabia, Yemen, and Iraq) implement the death penalty for same-sex relations, as do some provinces in Nigeria and Somalia.”); see also Patience Akumu, *Uganda: No Country for Gay Men*, THE GUARDIAN, Nov. 23, 2013, <https://www.theguardian.com/world/2013/nov/23/uganda-no-country-gay-men> (reporting that one couple could face two- and seven-year prison sentences after being outed and describing a proposed anti-homosexuality bill, supported by ninety percent of the public, which would impose the death penalty for some acts).

² See David Mizner, *The Saudi Monarchy's Harsh Crackdown on Dissent*, MSNBC, July 29, 2013, <http://www.msnbc.com/msnbc/the-saudi-monarchys-harsh-crackdown> (reporting the founder of a website criticizing the Saudi government was sentenced to seven years in prison and 600 lashes); see also Neil MacFarquhar, *Social Media Help Keep the Door Open to Sustained Dissent Inside Saudi Arabia*, N.Y. TIMES, June 15, 2011, <https://www.nytimes.com/2011/06/16/world/middleeast/16saudi.html> (“One weakness in online movements is that their organizers often stay hidden to avoid government wrath.”).

³ Roper, *supra* note 30.

⁴ Mike Levine & Jack Date, *22 Million Affected by OPM Hack, Officials Say*, ABC NEWS, July 9, 2015, <https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731>; Michael Adams, *Why the OPM Hack Is Far Worse Than You Imagine*, LAWFARE, March 11, 2016, <https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine>.

⁵ Nicole Perlroth, *State Department Targeted by Hackers in 4th Agency Computer Breach*, N.Y. TIMES, Nov. 16, 2014, <https://www.nytimes.com/2014/11/17/us/politics/state-department-targeted-by-hackers-in-4th-agency-computer-breach.html>.

III. Collecting Social Media Handles at the Border Will Cost an Extraordinary Amount of Time and Resources, Thus Constituting a Waste of Limited Government Resources.

Our concerns regarding the disproportionate consequences and burdens the visa questionnaire will impose on Muslims and people from Muslim-majority countries are further exacerbated by the fact that the Department’s Notices constitute a blatantly inefficient and ineffective expenditure of government resources. The Administration has not sufficiently addressed the enormous administrative burden that this collection will impose on applicants and U.S. officials, nor has it addressed the negligible national security benefit that will be gained in return. Because the Notices as written will not contribute to the Administration’s stated goal of more accurately identifying terrorism suspects, this substantial burden on travelers and the Department is unjustified.

A. The Notices Would Impose a Substantial New Burden on the Government Given the Scope of Data to be Analyzed and Effort Required to Garner Actionable Intelligence from Social Media Data.

The collection and analysis of social media identifiers for vetting and identity-resolution purposes will impose a substantial new burden on the Department. As noted above, the Department estimates the collection will impose a nearly twenty-three million hour burden on the agency. This estimate, though substantial, most likely understates the resources required to *effectively* make use of this new collection.

The Notices do not make clear the methodology the Department will use to examine the vast volume of additional information it gathers. Whether the analysis is conducted by the Department of State or another agency—for example, DHS—the Paperwork Reduction Act requires agencies to certify that they have allocated sufficient resources to process the information they collect in an efficient and useful manner.¹ The Department plans to use these accounts broadly for “identity resolution and vetting purposes based on statutory visa eligibility standards.”² However, the Notices do not contemplate the potential scope of applicant social media data. As we have noted in our previous comments, the average internet user has over five social media accounts—not only Facebook, Twitter, and Instagram, but also perhaps Badoo, Foursquare, LINE, LinkedIn, Myspace, OKCupid, Orkut, Pinterest, Qzone, Reddit, Sina Weibo, Snapchat, Tencent Weibo, Tinder, Tumblr, vkontakte, WeChat, and YouTube.³ Although only a specified list of social media handles will be required on the visa application form, applicants will be able to voluntarily provide additional identifiers. Given the high stakes at the border, many will inevitably feel obligated to provide as many as possible. This is particularly true given that the vast majority of other data fields in the questionnaire are mandatory. As a result,

¹ 44 U.S.C. § 3506(c)(3)(H).

² 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, 83 Fed. Reg. 13,807 (Mar. 30, 2018).

³ Shea Bennett, *The Average Internet User Has 5 Social Media Accounts*, ADWEEK (Oct. 24, 2014), <http://www.adweek.com/digital/social-media-accounts>; Marcelo Ballve, *Our List Of The World's Largest Social Networks Shows How Video, Messages, And China Are Taking Over The Social Web*, BUS. INSIDER (Dec. 17, 2013), <http://www.businessinsider.com/the-worlds-largest-social-networks-2013-12>.

applicants are likely to turn over their entire online presence to immigration officials. Despite this incredible volume of information, the Notices do not indicate if the Department will be checking every social media indicator provided or how it might prioritize certain accounts or platforms to make the process more efficient.

The Notices also provide no guidance on how long the information will be retained, leaving open the possibility that the data will be retained indefinitely. Expenses will be incurred in buying and maintaining the systems to store this information, as well as maintaining the security required to keep the information secure.

The Department also fails to acknowledge the vast resources required to effectively analyze social media data on a mass scale. Numerous studies show that bulk communications collection is an unreliable method for identifying terrorism suspects.¹ The collection proposed in the Notices would not only dramatically increase the documentation consular offices worldwide must sift through, but also would require examination by government employees with the requisite knowledge and training to interpret the collected information correctly. Even assuming, for the sake of argument, that a person’s social media presence can accurately convey whether they pose a threat to the United States—which, as explained further below, no evidence supports—adequate interpretation of social media information would require a substantial increase in personnel with sufficient language and cultural expertise to distill this information into “vetting” conclusions.² As highlighted above in Section II.A, without linguistic and cultural experts analyzing each application, an applicant’s social media presence may easily be misinterpreted—resulting in severe consequences for rejected applicants and a “false positive” for consular offices and the national security agencies with whom they share collected information.³ Unfortunately, none of these factors have been publicly accounted for by the Department, nor has its time estimate been broken down to describe what it actually includes.

B. Collecting Social Media Handles Will Be Ineffective at Identifying Terrorism Suspects, Will Duplicate Current Vetting Practices, and Will Have Substantial Economic and Foreign Policy Consequences.

1. The Proposed Collection Will Be Ineffective at Identifying Terrorism Suspects.

As proposed, the collection and analysis of social media profiles will be an unjustified use of federal resources because it will not yield actionable or accurate information. In fact, even DHS has recognized in internal documents detailing three prior uses of refugee social media

¹ See Anna Schmidt & Michael Wiegand, *A Survey on Hate Speech Detection Using Natural Language Processing*, Proceedings of the 5th International Workshop on Natural Language Processing for Social Media (2017), at 7, <http://www.aclweb.org/anthology/W17-1101> (“[T]here are much fewer hateful than benign comments present in randomly sampled data, and therefore a large number of comments have to be annotated to find a considerable number of hate speech instances. This skewed distribution makes it generally difficult and costly to build a corpus that is balanced with respect to hateful and harmless comments.”).

² See Duarte, *supra* note 33, at 14.

³ Press Release, Brennan Center for Justice, Tech Experts & Civil Rights Groups to DHS: Automated “Extreme Vetting” Would Be Threat to Constitutional Rights (Nov. 16, 2017).

accounts that “the information in [the social media] accounts did not produce clear links to national security concerns, even for those applicants who were found to pose a potential national security threat.”¹ As discussed above in Section II.A, when analyzed out of context, an applicant’s public social media profile is more likely to provide government agents with an inaccurate view of the applicant than provide valuable intelligence.

These risks are only heightened when the automated tools discussed above are used to analyze social media posts. The development of such an automated program would be costly and time-intensive, and there are well-documented roadblocks to the Department effectively using automated technology to analyze information it seeks in the Notices. First, automated systems do not operate with reliable accuracy. In one study, twenty different systems were used to evaluate “sentiment”—whether a user felt positively, negatively, or neutral about a given product.² These tools were successful only sixty-five to seventy-one percent of the time on average. They particularly struggled with jokes, sarcasm, and rhetoric. If these technologies fail to identify even three broad “sentiments,” they are not suitable for the more sophisticated analysis necessary for identifying threats to our country during the visa application process.

Further, this study did not even attempt to analyze non-English sources—and it is difficult to imagine that the Department has a plan to resolve this major issue in designing its own automated system. Even the most basic machine-based translation tools do not operate with sufficient accuracy to generate reliable translations, much less inferences based on those translations. Most commercially available natural language processing tools are only effective for English-language text, and will likely misinterpret non-English text.³

Finally, automated tools cannot be effectively applied across different social media platforms, subject matters, or languages, without significantly sacrificing their accuracy. To generate accurate outputs, these systems must be trained on and applied to data within a specific context. Researchers have had some limited success classifying text when their models are based on text from the same particular type of speech they analyze.⁴ However, these same tools cannot accurately classify different types of text, for example on different websites or in response to different types of events. For example, the way people use language to caption Instagram photos of their pets differs from how they use it to discuss political events on Facebook.⁵ Thus, a tool developed to analyze photo captions could not generate reliable insights

¹ Adolfo Flores, *People Are Worried About DHS Plans To Gather Social Media Info*, BUZZFEED NEWS, Sept. 28, 2017, <https://www.buzzfeed.com/adolfoflores/people-are-worried-about-dhs-plans-to-gather-social-media>.

² Abbasi, *supra* note 31, at 824, 829.

³ Duarte, *supra* note 33, at 12; *see also* 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, Et Al., *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>. (“[A]dequate training data . . . are not in abundance for languages other than English . . .”).

⁴ Duarte, *supra* note 33, at 4.

⁵ *Id.*



about the political conversations.¹ Language usage varies across platforms, types of conversations, and demography. Researchers studying sentiment analysis tools have found that tools trained on and applied to the same types of speech are eleven to fifteen percent more accurate than tools that are not.² The importance of training data on accurate identification was poignantly demonstrated by recent mistakes made by automated facial recognition tools developed by Google and Flickr. On several occasions, these tools misidentified African-Americans as apes.³ While similar to the examples of adverse impact of automation referenced in Section II, these errors also demonstrate the inaccuracies that arise from applying a tool trained on one set of data, in this case light-skinned faces, to other contexts.

Despite these well-known pitfalls, the Notices do not set forth any mechanism by which to evaluate the efficiency and accuracy of the collection and use of this information. Moreover, the Department has not indicated how vetting determinations at the border will be translated into actions by agents or adjudicators. If this program is to be implemented at all, meaningful oversight mechanisms should be built into it, including periodic audits and reviews as well as a formal dispute resolution mechanism for affected persons.

2. The Proposed Collection Will Duplicate Current Vetting Practice.

The Paperwork Reduction Act requires agencies to certify that their information collection is necessary for the proper performance of their functions, including showing that the information has practical utility and is not unnecessarily duplicative.⁴ The Department's Notices fail in this regard. First, the current vetting procedures on the books are already effective with respect to the Department's stated goals. A recent study from the CATO Institute found that current vetting failures are rare, especially since the attacks of September 11, 2001.⁵ In fact, according to the study only two percent of individuals convicted of terrorism offenses or killed while committing an offense in the United States since 9/11 entered due to a vetting failure. The study further clarified that it defined vetting failures broadly, to include failure to identify people who privately held extremist views before entering the country.

The Department has not demonstrated a need for additional layers of "extreme vetting," including the analysis of individuals' social media presence, on top of existing, effective procedures. Nor has it shown how its "extreme vetting" policy will vet travelers more thoroughly than the programs already in place to perform these tasks. The work of tracking

¹ *Id.* at 15.

² *Id.*

³ Jessica Guynn, *Google Photos Labeled Black People 'Gorillas'*, USA TODAY, July 1, 2015, <https://www.usatoday.com/story/tech/2015/07/01/google-apologizes-after-photos-identify-black-people-as-gorillas/29567465/>.

⁴ 44 U.S.C. § 3506(c)(3)(A).

⁵ See David Bier, *Extreme Vetting of Immigrants: Estimating Terrorism Vetting Failures*, CATO INST., Apr. 17, 2018, <https://www.cato.org/publications/policy-analysis/extreme-vetting-immigrants-estimating-terrorism-vetting-failures>.



foreigners who develop extremist views is primarily the responsibility of the FBI and other law enforcement agencies. These agencies have procedures in place based on decades of experience that have proven extremely effective and adaptable. Further, the Department’s collection and analysis effort may unnecessarily duplicate the DHS’s already troubling and unjustified “Extreme Vetting Initiative,” which is currently in development. It is unclear how the Department and DHS plan to coordinate their information collection efforts, whether or how they will share their collected information (and conclusions derived from it), and whether or how they will avoid needlessly collecting and analyzing multiple iterations of the same information from the same visa applicants. Building parallel systems with multiple expensive contracts would be a profound waste of government resources.

It is doubtful that the collection proposed by the Department will improve these efforts, because the requested information can be readily hidden or altered. Those seeking to enter the U.S., whether for nefarious or innocent reasons, can easily delete incriminating profiles or spend a few hours scrubbing their profiles of data that could compromise their chances of having their application approved—a practice routinely encouraged for millennials applying for jobs. Worse, applicants could create “dummy” accounts created specifically to undermine border officials’ investigations.¹ As a result, the Department’s proposal may actually deprive intelligence analysts of critical information by openly signaling that social media information is being regularly monitored and reviewed, thus inadvertently encouraging nefarious actors to sanitize their social media profiles or create false profiles that are expertly tailored to appear innocent and uncontroversial.

Meanwhile, most visa applicants who seek to enter the country for legitimate purposes may have a tendency to overshare any and all information that could be responsive to the questionnaire out of fear that failure to do so will result in rejection. This will add to the disproportionate burden on the Department with questionable intelligence yield.

3. The Proposed Collection Will Have Economic and Foreign Policy Costs for the United States.

Finally, the proposed information collection will have significant economic and foreign policy costs for the United States. Unlike the burdens discussed above in Section III.A, these costs are indirect consequences resulting from the implementation of this data collection, rather than costs directly imposed on the government. Adding unnecessary layers of inspection delays travelers’ entry into the country, which imposes a cost on the United States economy. Tourists will have less time (or will) to travel to and spend money in the United States. American businesses relying on members of the workforce who must retain visas will lose productivity, talent, and diversity. The Notices could lead to new burdens for American citizens traveling abroad, as well. Should foreign nations reciprocate this kind of social media information collection, Americans could be required to hand over their social media details, leaving them vulnerable to persecution in countries which lack the freedoms we enjoy.

Further, according to former U.S. intelligence officials, the Administration’s ineffective and inflammatory extreme vetting policies have made the United States less safe.² Policies that

¹ See Duarte, *supra* note 33, at 19–20.

² See Nina Totenberg, *Why Dozens Of National Security Experts Have Come Out Against Trump's Travel Ban*, NAT’L PUB. RADIO, Apr. 24, 2018 (quoting Gen. Michael Hayden, who served as director of the

throw useless hurdles in front of travelers, especially those that disproportionately affect Muslims, reinforce the narrative of extremist groups that the United States is at war with Muslims as a whole. They also weaken U.S. military and intelligence agencies' ability to recruit in conflict zones, as many Muslims in those areas cooperate with U.S. forces because they believe America is open to the Islamic faith, a position deeply undermined by the Administration's extreme vetting policies.¹

IV. Questions

Before embarking on this highly invasive, discriminatory, and wasteful program, the Department should be required to answer several key questions:

1. What gap is the Administration seeking to fill through these Notices? Would recent attacks on U.S. soil have been prevented by it?
2. What are the supporting policies and procedures for this program?
3. Will there be training in place to help prevent implicit or explicit biases from unduly influencing agents' decisions?
4. Will there be standards by which agents will have to determine whether to let someone in the country, or will it be purely subjective and based on "gut instinct"?
5. How many cultural/linguistic experts is the State Department hiring as part of this new information collection proposal?
6. What oversight mechanisms will be put in place to track the efficacy, cost, disparate impacts, and chilling effects of the data collection?
7. What complaint or dispute resolution process will be available to affected applicants?
8. How long will the Department store and maintain this data? Where will the data be stored?
9. With whom will the Department share this information domestically and globally?

National Security Agency from 1999 to 2005 and as CIA director from 2006 to 2009, writing that travel ban, "in addition to being unjust," has "actually made us less safe"), <https://www.npr.org/2018/04/24/604949251/why-dozens-of-national-security-experts-have-come-out-against-trumps-travel-ban>; see also Nick Miroff, *Trump is Creating a Vetting Center. Is It 'Extreme' Enough to End His Travel Ban?*, WASH. POST, Apr. 23, 2018, https://www.washingtonpost.com/world/national-security/trump-is-creating-a-vetting-center-is-it-extreme-enough-to-end-his-travel-ban/2018/04/22/6ab109fa-43fd-11e8-baaf-8b3c5a3da888_story.html.

¹ See Tottenberg, *supra* note 63 (quoting Gen. Michael Hayden: "It was the promise of America that allowed us to recruit people . . . just think of the impact of a pronouncement from the American government that people from that country, where you've just recruited, are never allowed . . . to enter this country.").

10. What cybersecurity measures will the Department implement to keep collected information secure and protected from being inadvertently disclosed?
11. How much will these Notices cost to implement?
12. Will automated tools be used to analyze this data? What are the accuracy rates of these tools? What are these tool's rates of false positive and false negatives and how will these results be handled?

Nothing in the Notice or the record surrounding this program suggests that the Department has answered or attempted to answer these questions. The answers to these questions would, as laid out above, make plain the inadequacy of the Notices' proposals and reveal the arbitrary and capricious nature of the entire program. Any final Rule that fails to address these questions would thus be incomplete.

V. Conclusion

The Department's proposal to make nearly every visa applicant answer the supplemental questionnaire is a costly and ineffective system offering only speculative, unlikely intelligence benefits. It would have a tremendous chilling effect on applicants' free speech and association on social media platforms, and will put vulnerable individuals at risk if their information is shared outside of the Department. Moreover, the Notices' negative effects would continue to disparately impact Muslims and individuals from Muslim-majority nations, further embedding the growing religious biases into our visa screening procedures. Muslim Advocates strongly urges OMB to reject the Department's request.

Respectfully submitted,

Matthew W. Callahan
Staff Attorney
Muslim Advocates