To: PRA_BurdenComments@state.gov [1]

Title of Information Collection: Supplemental Questions for Visa Applicants
OMB Control Number: 1405-0226
Form Number: DS-5535

Subject: DS-5535: Please do not renew

Privacy International comments on the Supplemental Questions for Visa Applicants, to ask you to not renew / extend the requirement for visa applicants to provide five years of social media handles.

Whilst we have concerns in relation to other proposed requested information, we focus these submissions in particular on the request for **"social media platforms and identifiers, also known as handles, used during the last five years."**

We note there is a lack of clarity including:

- What social media platforms will be targeted;
- What identifiers will be targeted and is there a definition used by officials for 'handles';
- Does this include both personal and work related or other shared social media activities;
- Will this permit searching of both 'public' and 'private' information and interactions i.e. will it include activities only visible to validated friends and direct messaging;
- By what methods is information provided processed, is it retained, when is it deleted;

We believe the rule, commenced under emergency approval earlier this year and for which now an extension is sought, is neither necessary nor proportionate for the stated aims of this measure - evaluating 'applicants for terrorism, national security-related, or other visa ineligibilities.' The use of social media intelligence (SOCMINT), the techniques and technologies used to monitor social media networking sites such as Twitter and Facebook, represents a significant intrusion into individual privacy. Any use of SOCMINT must comply with the international principles of legality, necessity and proportionality.

The measure fails to consider the highly privacy intrusive nature of demanding this information and the risks associated with collection, retention, use and sharing of a person's personal data, under a regime that lacks transparency and effective safeguards.

There is no consideration of the dangers of normalising the use of SOCMINT with the resulting reciprocal effects for US citizens applying for visit visas, and the dangers

[1] https://www.regulations.gov/docs/Tips_For_Submitting_Effective_Comments.pdf

associated with other governments implementing or expanding SOCMINT practices both in relation to immigration and other forms of surveillance. By way of example:

- In the US, the company ZeroFOX came under criticism when a report they had shared with officials of the city of Baltimore was released. In the report the company showcased how its social media monitoring tool could monitor the riots that followed Freddie Gray's funeral (Freddie Gray was a 25-year old African American who was shot by police). The report identified 19 "threat actors" among them were two leading figures of the civil rights movement #BlackLivesMatter, qualified as "physical threat."[2]

- In Thailand, the Technology Crime Suppression Division not only has a 30-person team scanning social media for lèse-majesté – speaking ill of the monarchy – content but it is also encouraging citizens to report lèse-majesté content they find online.[3]

- NGO Reprieve reported in 2015 that Saudi Arabia threatened the death penalty for tweeting and warned that people could face execution for tweeting 'rumours'. Reprieve noted that in an article published online on October 2015 the state-backed Makkah Newspaper said that a "judicial source" at the country's Ministry of Justice had "confirmed to Makkah Online that the death penalty is the harshest of the penalties that can be enacted upon those who spread rumours which create civil discord, via social media platforms like Twitter".[4]

SOCMINT includes monitoring of content, such as messages or images posted, and other data, which is generated when someone uses a social media networking site. The information involves person-to-person, person-to-group, group-to-group and includes interactions that are private and 'public'.

It is through social media that we express our views, our opinions and our sense of belonging to communities. Different generations, communities and individuals have their own context-dependent idiosyncratic way of communicating on social media.

To permit the monitoring of social media is to give a deep understanding of our social interactions, our habits, our location and our daily lives. "Tweets" posted on mobile phones can reveal location data, and their content reveals individual opinions (including political opinions) as well as information about a person's preference, sexuality, emotional and health status. This allows a substantial picture to be built of a person's interests, connections, and opinions. Using social media handles, officials can map private associational ties and harvest personal information and connections.

---

[2] https://www.privacyinternational.org/node/1481

[3] https://www.privacyinternational.org/node/1481 & https://www.privacyinternational.org/node/935

[4] https://www.reprieve.org.uk/press/saudi-government-threatens-death-penalty-for-tweeting-reports/

The proposal indicates that the methods of analysing social media networking sites vary and include manual and automated review. It is unclear what these processes provide in relation to results of searches and queries of users and activities or types of content users post. We are concerned at the lack of transparency in respect of the use of manual and automated collection techniques and other unspecified 'forms of information technology'[5]. What role do they play in decision making and how can outcomes be challenged?

Automated decision-making, including through the use of profiling, poses significant risks. Particularly, since derived, inferred or predicted profiles may be inaccurate, or otherwise systematically biased, profiling may also lead to individuals being misclassified or misjudged. When profiling is used to inform or feed into a decision that affects individuals, the outcome of such decisions may result in harm. In the words of the UN Human Rights Council:

> *"automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights"*[6]

The collection and processing of social media information may lead unintended consequences and abuse. Given the context specific nature of social media it could lead to misconstrued communications being treated as nefarious and result in rejected visa applications with personal and economic impact.

The arbitrary nature of this power, granting officials the ability to deny visas based on their interpretations of an individual's social media history, could result in abuses by individual officers as well as the systematic targeting of certain ethnic and religious group. By way of example, the case of *Raza v. the City of New York* revealed how the New York police were systematically gathering intelligence on the Muslim communities and part of the surveillance involved SOCMINT. It is unclear how there can be guarantees against such abuses given the opaque nature of this power and in view of the lack of supervision and oversight.

The policy will have a chilling effect on freedom of expression. Social media intelligence does not just affect the person targeted: it affects all the people within their networks. While one may agree with having a "public" chat on a social networking site, it is a different matter if the person you are speaking to has their social media interrogated and collected by officials. Thus, a review of social media will not be limited to an individual, but extend to friends, relatives and business associates.

It is likely that tactics used by officials will affect US citizens, yet there is no apparent consideration of First Amendment rights. However, social media is by definition, social and not constrained by national borders. You may be unaware that the

---

[5] https://www.regulations.gov/document?D=DOS-2017-0032-0001

[6] **U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)**

individual you are having a conversation on social media is applying for a visa, and you may never know if your conversations were collected and processed by officials as a result. It is inevitable that social media about U.S. citizens and permanent residents 'associated' with foreigners on social media will be collected.

When arbitrary power is granted to officials to deny visas based on their interpretations of an individual's social media history, the chilling effect on free speech affects all internet users, who fear openly expressing personal or political views in case such rules could someday be made to apply to them.

It sends a message that at any point, governments could change the rules to make anything you have every tweeted or posted on social media a basis for making decisions about your ability to visit, work in, or move to another country. Internet users should not fear having to justify each tweet or Instagram post to an immigration official. If social media is monitored, this will not only have a chilling effect on interactions, people may curate their social interactions to manipulate the system, rather than expressing themselves freely.

We note the concerns raised by civil and human rights organisations when this measures was first proposed[7] which are set out in Annex A.

About Privacy International

Privacy International is a UK-registered charity that promotes the right to privacy at an international level. Established in 1990, Privacy International undertakes research and investigations into state and corporate surveillance with a focus on the technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of the US, the United Kingdom and Europe, including the European Court of Human Rights. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy. It also strengthens the capacity of partner organisations in developing countries to do the same.

We confirm that we have read the 'Tips for submitting effective comments' and believe that our submission is compliant.[8]

---

7 http://www.brennancenter.org/sites/default/files/analysis/State%20Dept%20Information%20Collection%20Comments%20-%2051817_3.pdf

8 https://www.regulations.gov/docs/Tips_For_Submitting_Effective_Comments.pdf

Annex A

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

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

May 18, 2017

Dear Sir/Madam:

The undersigned organizations write to express our serious concerns about the Department of State's proposed policy to collect additional information from immigrant and nonimmigrant visa applicants who have been determined to warrant additional scrutiny in connection with terrorism or other national security-related visa ineligibilities.

As an initial matter, the Department of State has not provided an adequate rationale for why expediting the regulatory review process and shortening the period for public comment is necessary. Moreover, as described below, the additional requirements impose significant burdens on visa applicants; are apt to chill speech and reveal private information about travelers that is irrelevant to their suitability for entry to the United States; reveal information about their families, friends and business associates in the U.S.; appear designed to discriminate against Muslim travelers; and are unlikely to contribute to national security.

I. Expedited Review of the Proposed Collection is Unwarranted

The Department of State has requested assessment of this proposed information collection request ("ICR") pursuant to the "OMB Emergency Review" process, which compresses the timeline for public comment submissions and rule adjustments prior to a policy judgment.[1] However, the Department has not provided an adequate justification for triggering this expedited process.[2]

Typically, a total of 90 days are provided for public comment on an agency's ICR.[3] When an initial *Federal Register* notice is published, the public has 60 days to provide comments, after which the agency makes appropriate revisions to its proposed collection.[4] Then, the agency submits the ICR for Office of Management and Budget ("OMB") review and publishes another

---

[1] *Frequently Asked Questions*, OFFICE OF INFO. & REG. AFF., OFFICE OF MGMT. & BUDGET, https://www.reginfo.gov/public/jsp/Utilities/faq.jsp (last visited May 11, 2017) ("Under certain circumstances, the PRA authorizes an agency to request that an ICR be granted 'emergency' review and approval by OMB.").
[2] *Id.*
[3] *Id.*
[4] *Id.*

Federal Register notice that initiates a second, 30-day comment period, after which OMB concludes its review of the proposed collection.[5] Here, the Department of State requests emergency approval, which will be valid for 180 days, but it has provided only 14 days for public comment.

The Department of State fails to adequately justify such acceleration of the rulemaking process. Under the Paperwork Reduction Act ("PRA"), a request for emergency review requires the agency to provide "an explanation of why (for example) the normal process will result in public harm or is not possible because of an unanticipated event."[6] The Department of State's justification provides: "Adhering to ordinary time frames for review of newly proposed information collections… would impede the purposes behind the presidential memorandum and its call for immediate steps including the proper collection of all information necessary to rigorously evaluate those applicants for potential visa ineligibilities."[7] This justification is conclusory; the Department of State's own actions suggest that it has not conceived of this ICR as urgent.

While the relevant presidential memorandum – which instructs the Secretary of State, the Attorney General, and the Secretary of Homeland Security to implement "heightened screening and vetting of applications for visas and other immigration benefits" – does use the phrase "immediate implementation," it further specifies that such implementation is to be done "as soon as practicable that in [the agencies'] judgment will enhance…screening and vetting…."[8] Though the Department of State now asserts that cutting 76 days from the standard period for public comment is essential to comply with the memorandum's instructions, it waited 53 days before requesting from OMB an emergency review of this ICR. The Department's declared urgency is further belied by media reports suggesting that details of the proposed implementation were envisaged as early as mid-March 2017.[9]

"As soon as practicable" should not mean that the significant burdens and civil liberties concerns raised by this ICR are overlooked; instead, they must be carefully considered prior to implementation of the ICR. This process requires a longer period for public comment and for the Department of State to consider the comments it receives.

II. The Proposed Collection Excessively Burdens Visa Applicants

The proposed information collection imposes excessive burdens on visa applicants. The notice proposes collecting 15 years' worth of details on certain applicants' travel, address, and

---

[5] *Id.*
[6] *Id.*
[7] Emergency Memo/Justification submitted to OMB (April 28, 2017), *available at* https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201705-1405-001.
[8] Presidential Memorandum for the Secretary of State, the Attorney General, the Secretary of Homeland Security (March 6, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/03/06/memorandum-secretary-state-attorney-general-secretary-homeland-security.
[9] Yeganeh Torbati, Mica Rosenberg & Arshad Mohammed, *Exclusive: U.S. Embassies Ordered to Identify Population Groups for Tougher Visa Screening*, REUTERS (Mar. 23, 2017, 11:17 AM), http://www.reuters.com/article/us-usa-immigration-visas-exclusive-idUSKBN16U12X (discussing State Department cables with similar language regarding implementation of the March 6 immigration Executive Order).

employment history, which will be time-consuming and potentially impossible to comply with. Furthermore, the request for social media data – "platforms and identifiers" – is fatally ambiguous and will have a deleterious impact on the speech and privacy of the applicants as well as the Americans with whom they communicate. We address each of these objections in turn.

a. Information Requested Will Be Difficult to Compile and Verify

Given the volume of information that visa applicants must already provide,[10] requiring the additional disclosure of travel, address, and employment history going back 15 years is overly onerous. It may be nearly impossible to "provide supporting documentation" to verify funding information and other details related to a trip from more than a decade ago. The requirement to disclose domestic travel history for 15 years may be even more difficult to meet, as domestic travel is common and few people keep supporting documentation. In these circumstances, applicants committed to providing precise and verifiable information will be discouraged from applying for visas. Even if such additional information is only to be collected from people that consular officers suspect have "been in an area while the area was under the operational control of a terrorist organization,"[11] the lengthier 15-year time period requested predates ISIS, which is a driving force behind these policy changes.[12]

The Department's estimate that the "Average Time Per Response" is 60 minutes, resulting in a "Total Estimated Burden Time" of 65,000 hours, therefore cannot be correct.[13] Digging up travel history and financing information going back 15 years, and potentially accompanying verifying documentation, could take days, if not weeks, and involve numerous visits or phone calls to accommodation and transportation providers. Even a Single Scope Background Investigation, the type of investigation required for a Top Secret security clearance, goes back only 10 years for information on finances, education, and professional activities, raising doubts about the necessity of 15 years' worth of information.[14]

b. Request for Social Media Information is Ambiguous

The request for social media information is problematic as well: the ICR's description of the data requested – "[s]ocial media platforms and identifiers, also known as handles, used during the last five years" – is insufficient to provide guidance on the scope of required disclosure, adding to the burden in attempting to answer that section of the application.[15] The term "social media platforms" is not defined. While popular social media services such as Twitter, Facebook, and

---

[10] Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 20,957, *available at* https://www.gpo.gov/fdsys/pkg/FR-2017-05-04/pdf/2017-08975.pdf ("Most of this information is already collected on visa applications but for a shorter time period, e.g. five years rather than fifteen years.").

[11] Supporting Statement for Paperwork Reduction Act (May 5, 2017), *available at* https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201705-1405-001.

[12] *See, e.g.,* supra note 9 (highlighting how State Department cables implementing extreme vetting procedures require "social media checks" on applicants who have ever been present in ISIS-controlled territory).

[13] *Id.*

[14] Jeffrey Bennet, *What is an SSBI?*, CLEARANCEJOBS.COM (Sept. 8, 2013), https://news.clearancejobs.com/2013/09/08/ssbi/

[15] Fed. Reg., *supra* note 10, at 20,957.

Instagram may be the most obvious targets, some definitions of social media include blogging and similar online activities. Are applicants meant to cast as wide a net as possible in their disclosures, and will an inadvertent failure to do so be used as a reason to deny their entry into the country?

Similarly, the proposed form to be completed by applicants asks for "[social media platforms and identifiers] for *all* accounts you have used."[16] This phrasing suggests that travelers who maintain multiple accounts on a single platform – perhaps a personal one and a professional one – will need to disclose all such accounts, raising the risk that they will be held accountable for all posts on a particular profile even when they exercise only partial control.

We are encouraged by the Department's explicit limitation on consular officers' authority in this proposal – specifically, the directive that adjudicating officers are to refrain from requesting applicants' social media passwords or from subverting other privacy safeguards.[17] However, such guidance is insufficient to overcome significant problems with the substance of this policy, as described in the next section.

c. The Proposed Collection Will Capture Information That is Difficult to Interpret and Chill Free Expression

The IRC assumes that social media information will assist in revealing potential terrorists applying for visas. This seems unlikely. For one thing, it is doubtful that an individual who promotes terrorism online will disclose information about the social media profile that he is using to do so, or will retain postings that might raise concerns in the eyes of consular officials.

Also, problems of interpretation are guaranteed to plague any review of social media postings. One need only look at the 2012 experience of a British citizen who was turned back at the border because DHS agents were concerned about his posting on Twitter that he was going to "destroy America" – slang for partying – and "dig up Marilyn Monroe's grave" – a joke.[18] Government agents and courts have erroneously interpreted tweets repeating American rap lyrics as threatening messages in several previous cases.[19] Greater difficulties are inevitable if the language used is not English.

This is to say nothing of the challenges posed by non-verbal communication on social media. On Facebook, for instance, users can react to a posting with a range of emojis.[20] The actual meaning

---

[16] Proposed Form DS-5535 ("Supplemental Questions for Visa Applicants"), *available at* https://www.reginfo.gov/public/do/PRAViewIC?ref_nbr=201705-1405-001&icID=226719.
[17] Fed. Reg., *supra* note 10, at 20,957.
[18] *See* J. David Goodman, *Travelers Say They Were Denied Entry to U.S. for Twitter Jokes*, N.Y. TIMES (Jan. 30, 2012, 1:03 PM), https://thelede.blogs.nytimes.com/2012/01/30/travelers-say-they-were-denied-entry-to-u-s-for-twitter-jokes/?mtrref=undefined.
[19] *See, e.g.*, Natasha Lennard, *The Way Dzhokhar Tsarnaev's Tweets Are Being Used in the Boston Bombing Trial Is Very Dangerous*, FUSION (Mar. 12, 2015), http://fusion.net/story/102297/the-use-of-dzhokhar-tsarnaevs-tweets-in-the-bostonbombing-trial-is-very-dangerous/; Bill Chappell, *Supreme Court Tosses Out Man's Conviction for Making Threat on Facebook*, NAT'L PUB. RADIO (June 1, 2015), http://www.npr.org/sections/thetwo-way/2015/06/01/411213431/supreme-court-tosses-outman-s-conviction-for-making-threats-on-facebook.
[20] *See* Sammi Krug, *Reactions Now Available Globally*, FACEBOOK NEWSROOM (Feb. 24, 2016), http://newsroom.fb.com/news/2016/02/reactions-now-available-globally/.

of these emojis is highly contextual, however. If a Facebook user posts an article about the FBI persuading young, isolated Muslims to make statements in support of ISIS,[21] and another user "loves" the article, is he sending appreciation that the article was posted, signaling support for the FBI's practices, or sending love to a friend whose family has been affected? Assuming it is even possible to decode the meaning, that could not be done without delving further into the user's other online statements, interactions, and associations, as well as the postings of those with whom he or she communicates, a laborious, invasive, and error-riddled process. Indeed, such ambiguity is already affecting domestic criminal proceedings, with dire consequences.[22]

A similar dilemma infects Twitter, whose users have even fewer options for interacting with a post: they may respond, retweet it (with or without a comment), or "like" it with a heart. A user may click the heart simply to mark a post for later review, but it could falsely signal to her followers – or more urgently, the U.S. government – that she agrees with the sentiment expressed.

This may be an especially serious issue for journalists, particularly those writing on conflict zones: when a foreign journalist "hearts" a provocative tweet from an ISIS follower to be able to find it again more easily for a piece of writing, will that be taken as support for the follower's positions? And will he or she then be called to account for every "heart" and "like"? How about for those who "follow" or are "friends" with them? Political scientists and other scholars will face similar quandaries. In light of the multitude of possible interpretations of both speech and non-verbal communication, consular officers will be able to exercise enormous, unchecked discretion when it comes to assessing foreign residents' suitability to enter the country and quizzing them about the meaning and significance of a range of expression.

As a result of both the information request and the ambiguity pervading interactions on social media, online speech – particularly of the political or religious variety – will inevitably be chilled. Visa applicants will surely sanitize their own postings and internet presence to ensure that nothing online would provide cause for further scrutiny or suspicion by a rushed consular officer. Even if these travelers do not have First Amendment rights, a system that potentially penalizes people for statements they make online due to misinterpretation is profoundly incompatible with core American constitutional values. It is also incongruent with the International Covenant on Civil and Political Rights, which guarantees "the right to freedom of expression," including the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[23]

Moreover, the fact that the notice states that this collection of information will not be used to deny visas on the basis of religion or political views, while commendable, is insufficient. The

---

[21] *See, e.g.*, Eric Lichtblau. *F.B.I. Steps Up Use of Stings in ISIS* Cases, N.Y. TIMES (June 7, 2016), http://www.nytimes.com/2016/06/08/us/fbi-isis-terrorism-stings.html; Murtaza Hussain, *Confidential Informant Played Key Role in FBI Foiling Its Own Terror Plot*, INTERCEPT (Feb. 25, 2015, 9:09 PM), https://theintercept.com/2015/02/25/isismaterial-support-plot-involved-confidential-informant/.

[22] *See, e.g.*, Ben Popper, *How the NYPD Is Using Social Media to Put Harlem Teens Behind Bars*, VERGE (Dec. 10, 2014), http://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison.

[23] G.A. Res. 2200A (XXI), International Covenant on Civil and Political Rights (Dec. 16, 1966), http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

point of the disclosure requirement, presumably, is for consular officers to view and assess the content of applicants' postings. It is hard to imagine that the religious and political views reflected in those postings will not be taken into account in practice, even if officers are on paper prohibited from doing so.

Finally, reviews of travelers' social media profiles will also likely reveal other personal information, including their connections to friends, relatives, and business associates in the U.S., potentially subjecting Americans to invasive scrutiny of their personal lives. This scrutiny may undermine the right to communicate anonymously as well, a right that is protected by the First Amendment and was called a necessary condition for free expression by the U.N. Special Rapporteur on Freedom of Expression.[24] Requiring visa applicants to disclose their online identities may enmesh American citizens' communications and sweep in large quantities of constitutionally protected speech.

III. The Proposed Collection Will Primarily Burden Muslims

The burdens detailed above would be substantial regardless of the faith or ethnicity of a visa applicant. But the history of these vetting procedures indicates that they will primarily burden Muslims, raising substantial concerns about targeting individuals on the basis of their religious beliefs.

The Department of State describes the anticipated respondents as "[i]mmigrant and nonimmigrant visa applicants who have been determined to warrant additional scrutiny in connection with terrorism or other national security-related visa ineligibilities."[25] It estimates that 65,000 respondents, or 0.5% of U.S. visa applicants worldwide, will be affected.[26] The *Federal Register* notice does not indicate the basis of this estimate and provides no guidance on how respondents will be chosen.[27] It is reasonable to infer, however, that this number is based on the number of individuals who apply for nonimmigrant visas from the six Muslim countries designated in the President's Executive Order 13780, which banned travel to the United States from Iran, Libya, Somalia, Sudan, Syria and Yemen. The ICR explicitly states that it implements that order,[28] key portions of which have been enjoined by federal courts.[29] Tellingly, in fiscal year 2015, approximately 65,000 nonimmigrant visas were issued to citizens from these six

---

[24] *Anonymity*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/anonymity (last visited May 11, 2017); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep., Human Rights Council, at 1, U.N. Doc. A/HRC/29/32 (May. 22, 2015), *available at* http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc. (concluding that "encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection").

[25] Fed. Reg., *supra* note 10, at 20,957.

[26] *Id.*

[27] *Id.* It says in general terms: "[c]onsular posts worldwide regularly engage with law enforcement and intelligence community partners to identify sets of post applicant populations warranting increased scrutiny."

[28] *Id.*

[29] *See, e.g.*, Matt Ford, *A Make-or-Break Moment for Trump's Travel Ban?*, ATLANTIC (May 8, 2017), https://www.theatlantic.com/politics/archive/2017/05/fourth-circuit-travel-ban-oral-arguments/525900/.

countries.[30] In other words, it appears that the administration – stymied in its efforts to directly ban travel from these countries on constitutional grounds – may have decided to implement the same policy through its vetting procedures.

The history of the vetting procedures also suggests the intent to target Muslims. Shortly after becoming the official Republican presidential nominee, Donald Trump rolled out a new plan: "extreme vetting" for Muslims entering the United States.[31] He proposed that the United States admit only those "who share our values and respect our people."[32] One campaign official explained that people who have "attitudes about women or attitudes about Christians or gays that would be considered oppressive" would be barred.[33] Department of Homeland Security officials have indicated that visa applicants could be queried about honor killings, the role of women in society, and legitimate military targets.[34] It is difficult to see the connection between a visitor's view of the role of women in society and terrorism, but the connection between such questions and criticisms of the rights of women in Muslim societies is plain.[35]

The Department of State's notice states that "[t]he collection of social media platforms and identifiers will not be used to deny visas based on applicants' race, religion, ethnicity, national origin, political views, gender or sexual orientation."[36] However, given the context in which this ICR arises, and because it is part of a broader "extreme vetting" framework aimed at Muslims, that assurance seems less than credible. At the very least, this proposed collection fortifies an infrastructure through which future discriminatory policies may be administered. We express our concerns with designating people as raising national security concerns based on their religious background. Such classification undermines the historical tradition of the U.S. as a pluralistic, welcoming country without making Americans any safer.

---

[30] An additional 14,397 arrivals from these six countries came as lawful permanent residents, including as family members of U.S. citizens and awardees of the diversity immigrant visa program, meaning that the roughly 65,000 non-immigrant arrivals accounted for more than 80 percent of visa-based arrivals in fiscal year 2015. *See* Phillip Connor & Jens Manuel Krogstad, *Six Countries Named in Revised Trump Travel Order Accounted for More Than 650,000 U.S. Entries Since 2006*, PEW RESEARCH CTR. (May 10, 2017), http://www.pewresearch.org/fact-tank/2017/03/10/six-countries-named-in-revised-trump-travel-order-accounted-for-more-than-650000-u-s-entries-since-2006/. Those who intend to become permanent U.S. residents are subject to more rigorous vetting, and must customarily provide additional information like affidavits of support, birth certificates, and medical examination results. *See The Immigrant Visa Process*, BUREAU OF CONSULAR AFF., U.S. DEP'T OF STATE, https://travel.state.gov/content/visas/en/immigrate/immigrant-process/interview/prepare/interview-preparation-required-documents.html (date visited May 11, 2017).

[31] Jeremy Diamond, *Trump Proposes Values Test for Would-be Immigrants in Fiery ISIS Speech*, CNN (Aug. 15, 2016, 9:39 PM), http://www.cnn.com/2016/08/14/politics/donald-trump-isis-fight/.

[32] *Id.*

[33] *Id.*; *see also* Deborah Amos, *Trump Backers Want Ideology Test for Extreme Vetting*, NAT'L PUB. RADIO (Feb. 4, 2017), http://www.npr.org/sections/parallels/2017/02/04/513289953/trump-backerswant-ideology-test-for-extreme-vetting (quoting a proponent of the executive order describing the extreme vetting process as instituting "a kind of ideological screening").

[34] Laura Meckler, *Trump Administration Considers Far Reaching Steps for 'Extreme Vetting'*, WALL ST. J. (Apr. 4, 2017), https://www.wsj.com/articles/trumpadministration-considers-far-reaching-steps-for-extremevetting-1491303602.

[35] Faiza Patel, *Reflections on the Prejudice in the Draft Exec Order's Vetting of 'Prejudice'*, JUST SEC. (Jan. 27, 2017), https://www.justsecurity.org/36898/reflections-prejudice-draftexec-orders-vetting-prejudice/; Faiza Patel & Erica Posey, *Beware Trump's Phony 'Terror' List,* DAILY BEAST (Mar. 22, 2017), http://www.thedailybeast.com/articles/2017/03/22/ beware-trump-s-phony-terror-list.html.

[36] Fed. Reg., *supra* note 10, at 20,957.

IV. There is No Evidence that Foreign Visitors Pose a Significant Threat to the U.S.

Lastly, there is ample evidence that foreigners as a group pose little security risk to this country.[37] According to the CATO Institute, which surveyed data from 1975 to the end of 2015, Americans have a 1 in 3.6 million chance of being murdered by a terrorist attack on U.S. soil that was committed by a foreigner (including the attacks of September 11), and a 1 in 3.64 billion chance of being killed in a terrorist attack committed by a refugee. In those same 41 years, 1 foreign-born terrorist entered the U.S. for 7.38 million other foreigners using the visa types those terrorists used; excluding the September 11 terrorists, this number was 1 for every 8.48 million. By comparison, Americans have a 1 in 14,000 chance of being murdered by anyone.[38] Indeed, national security arguments for the administration's attempts to ban Muslims and refugees from the United States have been refuted by more than 130 national security experts and viewed with great skepticism by several federal courts.[39]

V. Conclusion

For the above reasons, we urge the Department of State to abandon this proposed information collection initiative. Please do not hesitate to let us know if we can provide any further information regarding our concerns. We may be reached at patelf@brennan.law.nyu.edu (Faiza Patel: 646-292-8325), levinsonr@brennan.law.nyu.edu (Rachel Levinson-Waldman: 202-249-7193), or pandurangah@brennan.law.nyu.edu (Harsha Panduranga: 646-292-8719).

Sincerely,

18MillionRising.org
Advocates for Youth
American-Arab Anti-Discrimination Committee
Americans United for Separation of Church and State
Asian Americans Advancing Justice
Brennan Center for Justice at NYU School of Law
Center for Constitutional Rights
Center for Democracy & Technology
Center for Media Justice
Committee to Protect Journalists

---

[37] ALEX NOWRASTEH, CATO INST., NO. 798, TERRORISM AND IMMIGRATION: A RISK ANALYSIS (Sept. 13, 2016), *available at* https://www.cato.org/publications/policy-analysis/terrorism-immigration-risk-analysis.
[38] *Id.*
[39] Lara Jakes, *Trump's Revised Travel Ban Is Denounced by 134 Foreign Policy Experts*, N.Y. TIMES (Mar. 11, 2017), https://www.nytimes.com/2017/03/11/us/politics/trump-travel-ban-denounced-foreign-policy-experts.html; Lawrence Hurley, *Judges Hit Trump Lawyer With Tough Questions Over Revised Travel Ban*, REUTERS (May 6, 2017, 7:30 PM), http://www.reuters.com/article/us-usa-immigration-court-idUSKBN1840ZU. Relatedly, claims that terrorism-related offenses have been committed primarily by foreigners have been labeled as misleading by expert analysts. *See* Miriam Valverde, *Trump Misleads in Claim About Terrorism Convictions Since 9/11*, POLITIFACT (Mar. 2, 2017, 1:41 PM), http://www.politifact.com/truth-o-meter/statements/2017/mar/02/donald-trump/trump-misleads-claim-about-terrorism-convictions-9/; Andrew Lindsay, *What the Data Tells Us About Immigration and Terrorism*, BRENNAN CTR. FOR JUSTICE (Feb. 17, 2017), https://www.brennancenter.org/blog/what-data-tells-us-about-immigration-and-terrorism.

Council on American-Islamic Relations (CAIR)
Defending Rights & Dissent
Electronic Frontier Foundation
Free Press Action Fund
Human Rights Watch
Iranian American Bar Association
Legal Aid Justice Center
MPower Change
Muslim Alliance for Sexual and Gender Diversity, MASGD
Muslim Justice League
National Hispanic Media Coalition
National Immigration Law Center
National Immigration Project of the National Lawyers Guild
National Iranian American Council (NIAC)
National Network for Arab American Communities
New America's Open Technology Institute
New York State Immigrant Action Fund
Resilient Communities Program of New America
Restore The Fourth
Services, Immigrant Rights, and Education Network (SIREN)
South Asian Americans Leading Together (SAALT)
Southern Poverty Law Center
United Church of Christ, Office of Communication, Inc.
World Privacy Forum
Yemen Peace Project