

October 2, 2017

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

RE: Supplemental Questions for Visa Applicants, OMB Control Number 1405-0026, DS-5535
Docket Number: DOS-2017-0032

To Whom It May Concern:

The American Civil Liberties Union (ACLU) submits these comments in response to the Department of State (Department) *60-Day Notice of Proposed Information Collection: Supplemental Questions for Visa Applicants*. The ACLU opposes the proposed questions in the notice and urges the Department to abandon them in their entirety. Since issuing the emergency notice regarding this proposal in May, the Department has made few to no changes to the supplemental questions and provides no further information or parameters to limit their overly broad and burdensome nature. The proposed questions still needlessly expand the information sought from approximately 65,000 visa applicants each year, slowing the visa application process, raising constitutional concerns regarding the rights to due process, free speech, and expression, and impacting the privacy of millions of living in the United States, including U.S. citizens.

The Department seeks to continue asking overly broad and burdensome questions of immigrant and nonimmigrant visa applicants by reaching further back into their travel, address, and employment histories; requiring information regarding siblings, children, spouses, and partners; and looking into their social media activities. Furthermore, the proposed questions do not include any standards or guidance regarding who will be asked these questions, thereby increasing the likelihood of inconsistent and ineffective determinations as well as bias and unlawful profiling within these visa adjudications. Finally, the notice provides no definitions or parameters with respect to the social media question, creating substantial concerns regarding the meaning or purpose of the question; the substantial impact of the question on privacy, due process rights, and freedom of speech and expression of individuals in the United States, including U.S. citizens; and the use, storage, and retention of the information collected about visa applicants and individuals living in the United States.

We urge the Department to abandon the proposed questions in their entirety. Despite the fact that months have passed since the emergency notice, the Department provides no further information or parameters regarding these questions or the use of data obtained. At a minimum, the

Department must withdraw the current notice and seek expanded public comment through notice of proposed rulemaking, providing guidance as to who will be asked the questions, definitions regarding the terms, and details as to how the rights of individuals living in the United States, including U.S. citizens, will be protected as well as how the information will be used and stored.

I. The proposed questions are overly broad and burdensome.

The proposed questions seek information from applicants about their last 15 years of travel history, address history, and employment history as well as passport numbers for foreign passports, names and dates of birth for siblings, children, and current and former spouses or civil or domestic partners, and social media platforms, identifiers, phone numbers, and email addresses used by the applicant in the last five years.¹ Such questions clearly go beyond what is relevant or necessary to protect national security. Additionally, the notice states that applicants will be asked the details of their travel, including domestic travel, if the consular officer believes they “have been in an area while the area was under the operational control of a terrorist organization.” Visa applicants will also be asked for the “source of funding” for their travel for the last fifteen years.

There is no rationale provided for asking any of these questions, nor does the Department specify how this information will be used despite the months that have passed since the emergency notice. When and how will officers decide that information dating back 15 years needs to be acquired? How will an officer determine that it “appears” that the applicant was in a region which was under the operational control of a terrorist organization while the applicant was there? What funding will be assessed as legitimate and what will be suspect? How will officers be applying these standards? What training will they have regarding these new questions? By requiring that applicants provide this information for the last 15 years, these questions will make the application process more burdensome for applicants and will result in longer adjudication times and processing delays without any basis, rationale, or guidance as to how the information will be used.

The Department’s notice also includes questions regarding “social media platforms and identifiers, also known as handles” used for the last five years. However, it provides no definitions for these terms. These terms must be defined more precisely in order for an applicant to understand how to answer adequately and so that the public better understands the scope of information to be collected and analyzed by the government. Terms such as “platform” and “identifier” can be interpreted broadly or narrowly, and “social media” is itself a broad term as well. It is not clear whether the Department intends this to include more obvious and frequently used platforms in the United States such as Facebook and Twitter, or whether it includes blogs or video game, health, or dating applications as well. In order for applicants to answer these questions and for the public to understand the reach of the government into their personal habits, choices, beliefs, and expression, the Department must provide clarity regarding the scope of the information it is requesting.

The notice also indicates that the failure to provide responses to the proposed questions would “not necessarily result in visa denial” if the officer determines that the applicant has provided a

¹ Questions related to social media activities are discussed separately in Part III.

credible explanation for not providing the information. It is not clear what qualifies as a credible explanation. For example, if an individual does not remember a trip from 14 years ago or the “source of funding” for the trip, or does not wish to provide a social media handle or does not remember one, will the visa be denied? If an individual provides information that is later determined inaccurate because they did not remember details, will they be at risk of prosecution under existing laws if they are admitted? The notice provides no guidance on these questions.

Although we raised these questions in our comment on the initial notice months ago, the Department has provided no further guidance as to the purpose of these questions, definitions of the terms used, use of the information gathered, or the impact of not providing the information. The only legitimate way for the Department to propose the collection of this information is through proposed notice and rulemaking subject to public comment, which must include definitions for these terms, the scope of the information being collected, and the ways in which it will be used so that the public may adequately comment.

II. The lack of standards governing who will be asked these additional questions will likely result in inconsistent and ineffective determinations as well as discriminatory profiling.

According to the notice, immigrant and nonimmigrant visa applicants “who have been determined to warrant additional scrutiny in connection with terrorism or other national security-related visa ineligibilities” will be asked these new questions. However, the notice still sets out no basis or standards by which the Department will make such determinations. The Department alleges that approximately 0.5% of visa applicants, or 65,000 applicants annually, will “present a threat profile” that will necessitate the collection of this information. It further states that applicants will be asked the details of their travel if the officer believes they “have been in an area while the area was under the operational control of a terrorist organization.” Without any further elaboration or detail as to how these determinations will be made, these proposed questions are extremely vague and broad, making them likely to result in arbitrary, inconsistent, and ineffective determinations.

Furthermore, this notice cites its purpose to continue the implementation of the President’s directive, referencing President’s Memorandum for the Secretary of State, the Attorney General, and the Secretary of Homeland Security on heightened screening and vetting of applications for visas and other immigration benefits.² That memorandum in turn cited Executive Order 13780, also signed on March 6, 2017, which barred individuals from six Muslim-majority countries and refugees.³ The President issued that Executive Order, upon which the Memorandum and Federal

² Memorandum for the Secretary of State, the Attorney General, and the Secretary of Homeland Security, *Implementing Immediate Heightened Screening and Vetting of Applications for Visas and Other Immigration Benefits, Ensuring Enforcement of All Laws for Entry into the United States, and Increasing Transparency among Departments and Agencies of the Federal Government and for the American People* (March 6, 2017) available at <https://www.whitehouse.gov/the-press-office/2017/03/06/memorandum-secretary-state-attorney-general-secretary-homeland-security>.

³ Executive Order Protecting the National from Foreign Terrorist Entry into the United States (March 6, 2017) available at <https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states>.

Register notice are based, in an attempt to single out and condemn Muslims. Given this discriminatory premise and the vague language in the notice, the proposed questions heighten the likelihood of discriminatory profiling in visa determinations and the unjust targeting of people of particular faiths or national origins. Executive Order 13780 and its predecessor, Executive Order 13769, were an attempt to implement President Trump’s pledge to target Muslims, using national origin as a proxy.⁴ It must also be noted President Trump has repeatedly called for “ideological certification” and “extreme vetting” while making specific reference to Islam, Muslims or people from Muslim-majority countries, conflating these categorically with terrorism.⁵ Additionally, other programs and policies, such as those used to conduct surveillance and watchlist people, have used similarly vague terminology resulting in the unjust discriminatory treatment of Muslim, Arab, Middle Eastern, and South Asian communities. Adding an unjustified layer of screening without any basis or standard would likely subject these communities to further discrimination.

By failing to articulate standards for imposing such additional questioning or how the information will be used, the Department creates the risk of inconsistent and ineffective determinations and heightens the threat of discrimination and profiling of visa applicants.

III. The notice lacks parameters or guidance regarding the request for social media information.

The Department has proposed a social media-related question, requesting “social media platforms and identifiers, also known as handles, used during the last five years.” The notice provides no other information regarding the definitions of these terms or how the information will be stored, retained, or used; this includes both the information searched, reviewed, and collected of applicants as well as individuals living in the United States, including U.S. citizens, who might be connected to applicants. Several months after the emergency notice, the current notice simply requires that consular staff “avoid collection of third-party information,” providing no detail or guidance with respect to what “collection” means, how such collection will be avoided, or how any collection of such information that does occur will be addressed. To the extent the Department plans to make use of the social media platforms and identifiers it collects by visiting those platforms to view statements and associates of the applicant on them, it seems impossible for the Department to avoid viewing and collecting third-party information. Indeed, the entire function of social media platforms is to allow connection and communication between an individual user and third parties.

⁴ See also Presidential Proclamation Enhancing Vetting Capabilities and Processes for Detecting Attempted Entry into the United States by Terrorists or Other Public-Safety Threats (September 24, 2017) (indefinitely barring certain individuals from six Muslim-majority countries as well as a small number of individuals from two additional countries), available at <https://www.whitehouse.gov/the-press-office/2017/09/24/enhancing-vetting-capabilities-and-processes-detecting-attempted-entry>.

⁵ See Los Angeles Times Staff, *Transcript: Donald Trump’s Full Immigration Speech* (Aug. 31, 2017) available at <http://www.latimes.com/politics/la-na-pol-donald-trump-immigration-speech-transcript-20160831-snap-htmstory.html>; Rebecca Shabad, *Donald Trump Calls for “Extreme” Ideological Screening Test for New Immigrants* (Aug. 15, 2016) available at <http://www.cbsnews.com/news/donald-trump-proposes-ideological-test-immigration-u-s/>.

As recently as February 2017, the Office of the Inspector General (OIG) issued a report concluding that the Department of Homeland Security's (DHS) social media screening pilot programs do not have clear success criteria, and that DHS therefore may not be able to design an effective social media screening program.⁶ The OIG also recommended that DHS develop and implement "well-defined, clear, and measurable objectives and standards" to evaluate its social media screening pilot programs.⁷ The Department must develop similar standards for these questions as a part of the notice process so that the public has a meaningful opportunity to comment.

A. Officer assessments will be subjective and based upon unreliable or circumstantial evidence.

According to the notice, the proposed questions seek to "resolve an applicant's identity or to vet for terrorism or other national security related visa ineligibilities" where there is a need for enhanced scrutiny. However, the lack of clarity in the questions, definitions of terminology, the scope of the information to be collected, and the ways in which it will be used make the collection of this information unreliable and subject to abuse. The decision-making regarding visas will itself become more uncertain because it will involve a wide array of social media information about applicants as well as other individuals.

Moreover, decision-making based on social media information will inevitably be subjective. In evaluating applicants' responses to the social media question, officers will determine whether applicants are worthy of visas without limitations or guidelines regarding how to interpret such information. This subjective decision-making process would offer little or no opportunity to learn the basis for a denial and no transparency about the information being collected on applicants and their U.S.-based contacts and correspondents. In sum, it would add a layer of scrutiny to certain visa applicants without articulable basis, yielding complex, wide-ranging, capricious, politically charged, and highly subjective assessments without providing detail or standards as to how the assessments will be carried out.

B. Information will be gathered about millions of individuals living in the United States without their consent, impacting their First Amendment rights of free speech and association.

Given that the Department is collecting a broad swath of information that is poorly defined and lacking clear guidelines for use, such collection will enable the Department to search the internet for an applicant's contacts, and to view communications between applicants and their contacts. Inevitably, this information will include the identities and communications of those living in the United States, including U.S. citizens, who are connected in some fashion to the visa applicant. This nonconsensual collection of information about people in the United States raises serious First Amendment concerns because it threatens to chill protected speech and associational activities.

⁶ Office of Inspector General, *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-Term Success (Redacted)*, OIG-17-40 (Feb. 27, 2017) available at <https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf>.

⁷ *Id.*

The current notice directs consular staff to “avoid collection of third-party information.” It does not prohibit the search or review of third-party information, nor does it provide any guidance regarding what “collection” means, and whether that simply means the government will not store the data, or how any review or collection of such information that does occur will be addressed. Despite the significant privacy, free speech, and associational concerns for individuals living in the United States, including U.S. citizens, the Department seeks to resolve this issue with one new line in its notice.

According to the notice, approximately 65,000 applicants will be affected annually, which means there are likely to be millions of U.S.-based contacts, the vast majority of whom have done nothing to cause the government to scrutinize their actions and communications and all of whom will have done nothing to consent to the search or review of their personal information.

The Department’s proposed questions request information regarding visa applicants’ social media platforms and identifiers. Any use of this information by the Department would result in the review and collection of a massive amount of personal communications and information about the individuals with whom the applicants are communicating. It will result in the Department deriving data on millions of contacts—many of them U.S. citizens—who happen to be connected to the applicant by social media, whether as a friend on Facebook, a follower on Twitter, or perhaps a match on a dating application or website. Through this mechanism, information would be searched and reviewed on anyone living in the United States, including U.S. citizens, without their knowledge.

Collection of this information raises several First Amendment concerns. First, it will chill freedom of association by allowing the government to chart and amass the connection of individuals living in the United States, including U.S. citizens, to applicants and to each other. This is a particular concern when people are associating online around controversial political viewpoints. It also threatens to impinge on the right to engage in anonymous speech and association. Individuals are generally not required to use their actual names on social media platforms, and may have non-identifying or pseudonymous handles, including to protect their privacy or to shield themselves from retaliation or persecution for espousing unpopular views or supporting controversial causes. When an applicant provides information about a handle that they have used without previously disclosing their actual identity, their contacts, who may not have otherwise been known to have been communicating or associating with the applicant, will become targets of government scrutiny.

Second, even when the Department is collecting and viewing information that is publicly available on social media platforms, the ability to aggregate and review all connections and communications of applicants across multiple social media platforms raises unique concerns that may chill individuals’ in the United States willingness to engage in association and dialogue online. This scrutiny may encourage U.S. citizens and others living in the United States to be more circumspect in connecting with those outside the United States.⁸ To the extent an

⁸ See PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (Nov. 12, 2013); Karen Turner, *Mass Surveillance Silences Minority Opinions, According to Study*, Wash. Post, (Mar. 28, 2016) available at <https://www.washingtonpost.com/news/the->

individual can control to whom they are connected online, anyone who is concerned about personal privacy or anyone who is reluctant to share personal beliefs or comments with government investigators will be less likely to engage online. Whether in large or small degree, it will chill law-abiding individuals in the United States, including U.S. citizens, from engaging in online activity. Instructing officers to “avoid collection” of their data will do little to protect against a chilling effect, particularly since there is no explanation of what it means to avoid collection or whether the information of U.S. citizens or residents will be searched, reviewed, and shared with other agencies or components.

Government investigation of individuals should be based on facts and evidence—not through random identification based upon contacts. For government to target, search, and review third-party data without reason or basis creates a broad scale, unwarranted threat to constitutionally protected rights. The Department has provided no parameters or limitations to any search, review, or collection of information.

For the Department to move forward with dramatic changes to the visa process that result in information collection impacting millions of individuals living in the United States, including U.S. citizens, without providing adequate information poses incredible risks to the privacy and freedom of speech and association of individuals nationwide.

C. The Department has provided no information about how information might be shared or used by other agencies or their components.

The Department has provided no information or assurance regarding how the information provided by the applicant or any third parties information might be used by other agencies or their components, denying applicants the ability to make informed decisions about their submission and creating constitutional concerns for everyone living in the United States, including U.S. citizens.

As mentioned previously, applicants have not been provided guidance regarding the impact of not providing certain information on their applications, even when they do not remember. For example, they do not know what qualifies as a “credible explanation” for not providing social media information, so declining to provide this information may in fact result in the denial of their applications for admission. This poses a Hobson’s choice, against which an applicant must weigh potentially urgent necessity for a visa—e.g., to attend school, to attend a business meeting, or to visit or join family in the United States. The Department has not provided information sufficient for an applicant to make that decision or for the public to understand and comment on the government’s reach into applicants’ lives. Based upon this notice, applicants have no idea how the information they provide might be used by other agencies or components—such as the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), or even local law enforcement—once the applicants enter the United States. They do not know how their information will be shared or used to monitor or conduct surveillance of themselves, their families or friends, or other third parties, and therefore, they cannot make an informed decision

about whether to submit the information, state that they are declining to submit the information, or withdraw the application for admission.

Additionally, the third parties themselves do not know their information is being searched, reviewed, and possibly shared with other agencies and components. Millions living in the United States, including U.S. citizens, will be third parties in this visa application process, thereby subjecting their information to potential use by the FBI, ICE, local law enforcement, or other agencies and components without their knowledge or consent. Moreover, the notice provides no clarity regarding how the Department intends to comply with existing privacy laws, such as the Privacy Act or Judicial Redress Act, which provide certain protections for U.S. citizens, green card holders, and some non-U.S. citizens.

As a part of the public comment process, the Department must provide applicants and the general public—which includes the countless potential third parties whose private information may be searched and shared—with clarity regarding the use of information both within the application process and for the foreseeable future. To obtain and use this information without the consent or even awareness denies applicants the ability to make an informed decision regarding whether to submit a visa application and raises serious constitutional concerns for individuals living in the United States, including U.S. citizens, nationwide.

D. There is no guidance or plan regarding the use, storage, or retention of the information collected.

The notice does not indicate how the data of visa applicants and individuals living in the United States, including U.S. citizens, will be used, stored, retained, or shared with other agencies across government or private entities. Any proposal with such a substantial impact on our immigration processes and constitutionally protected rights must address how the data derived from social media identifiers will be collected, disseminated, and retained, so that the public may have an opportunity to comment.

Regarding visa applicants, the Department provides no guidelines regarding how any information collected will be used or when the requested information will result in the denial of a visa. In theory, the Department might exclude an applicant based on information gleaned from social media contacts, “likes” of particular statements or articles, retweets of others’ statements, or even online purchases. There is no information as to whether the Department will assess an individual’s social media comments, contacts, evidence of travel or studies, or professional achievements or failures. Based upon the notice, the applicant will not know what information has been collected or how it is being perceived or used, which also means that the applicant has no way of rebutting false presumptions or information interpreted out of context. Equally unclear is how the applicant’s social media contacts’ information will be used and whether they will also be scrutinized, logged, and monitored by the government regardless of having applied for an immigration benefit or whether they are living in the United States, including U.S. citizens. Without such guidance, we are left to assume that applicants could be excluded even if they are unaware of an indirect connection to someone who is considered suspect.

If such a denial occurs due to information gleaned from social media identifiers, it remains unclear if the applicant will have an opportunity to correct any erroneous, misleading, or unsubstantiated information derived from the identifiers that generated the denial. Aside from the personal or business impact on the applicant's travel plans, the retention of any such corrupted information within any databases maintained by the Department or other governmental entities could cause similar or other incorrect decisions in other circumstances. Having a meaningful opportunity to correct the record will benefit not only the applicant, but also the reliability of the information on which the government depends in carrying out its mission.

For individuals living in the United States, including U.S. citizens, who are caught up in this data collection, it will be even more difficult to make sure the government is not drawing incorrect conclusions about their contacts and activities. The notice makes no reference to its intended plans for the information derived from researching the social media identifiers. Simply directing officers to "avoid collection" of data regarding third parties is insufficient. If the Department or another agency identifies individuals living in the United States through the use of social media identifiers provided on a visa application, it should promptly purge any record of that person's identifiable information. It should also make clear that that information will not be used in any immigration adjudication of that third-party nor stored or retained by other agencies or components. If the information is reviewed and used in the adjudication, the government should provide notice to that U.S. person as well as an opportunity to verify that the information is accurate and to challenge its inclusion. Failure to provide such an opportunity would undermine the rights of millions of people living in the United States, including U.S. citizens. The Department must provide that plan and offer an opportunity for public comment.

The Agency must provide detailed information on its plan to allow applicants to collect information derived from using social media identifiers and on its plans to retain and share information on those living in the United States, including U.S. citizens, and offer an opportunity for public comment.

E. There will likely be a chilling effect on trade, commerce, and interaction with the United States and those living in the United States, including U.S. citizens.

Individuals decide to travel to the U.S. for many different reasons—to engage in business, visit family, speak at a conference, or pursue an education, to name a few. Certainly tourism is one of the leading draws of foreign visitors and a leading economic driver in many parts of the country. Each such visit has a discrete and tangible economic and cultural benefit—both to the country and often to the visa applicant as well. Any action that would make such visits less attractive to the traveler or less likely to occur is one that should be discouraged. By asking visa applicants to reveal their social media identifiers, with the understanding that the U.S. government will be examining their online activity and contacts, we are making our country less hospitable and we are making our visitors more likely to be secretive or to forgo travel to the United States, even if their activities pose no threat to our country.

Furthermore, anyone actually engaged in terrorism will simply take additional steps to hide their communications, making this information collection ineffective. There will be relatively little to gain from such a process and a massive impact on our immigration system and processing as

well as the rights of the U.S.-based contacts of these applicants who wish to engage with them once they arrive in the country.⁹

We urge the Department to seek public comment on the anticipated impacts of the proposal on the speech and association rights of individuals living in the United States, including U.S. citizens, and how the chilling effect of the proposal might harm American business, tourism, cultural institutions, and other national interests.

IV. Conclusion

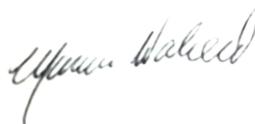
The Department's proposed supplemental questions are problematic, procedurally and substantively. Rather than publishing a proposed notice of rulemaking for this expansion of visa processing, the Department still fails to provide any guidance or parameters regarding these questions, months after the emergency notice was published and put into effect. These proposed questions reach deep into the histories of visa applicants without any parameters or guidance regarding when, how, and to whom these questions will apply, creating an environment ripe for profiling and discrimination. The Department states no plan for the use, storage, or retention of this information and disregards the constitutionally protected rights of millions living in the United States, including U.S. citizens.

The ACLU opposes the proposed questions in the notice and urges the Department to abandon them in their entirety.

Sincerely,



Faiz Shakir
National Political Director



Manar Waheed
Legislative and Advocacy Counsel

⁹ See *Kleindienst v. Mandel*, 408 U.S. 753 (1972) (recognizing that people and organizations in the United States have First Amendment-protected interests in receiving information from people seeking a visa to enter the country); *American Academy of Religion v. Napolitano*, 573 F.3d 115 (2d Cir. 2009) (same).