

**Before the**  
**BUREAU OF CONSULAR AFFAIRS**  
**VISA OFFICE (CA/VO/L/R)**  
**U.S. DEPARTMENT OF STATE**  
**Washington, DC 20520**

---

60-Day Notice of Proposed  
Information Collection: Application for  
Nonimmigrant Visa, Forms DS-160  
and DS-156, OMB Control Number  
1405-0182, Docket Number DOS-  
2018-0002, FR Doc. 2018-06496

and

60-Day Notice of Proposed  
Information Collection: Application for  
Immigrant Visa and Alien Registration,  
Form DS-260, OMB Control Number  
1405-0185, Docket Number DOS-  
2018-0003, FR Doc. 2018-06490

**COMMENTS OF THE IDENTITY PROJECT (IDP),  
GOVERNMENT INFORMATION WATCH,  
CYBER PRIVACY PROJECT (CPP), AMERICAN  
ARAB ANTI-DISCRIMINATION COMMITTEE  
(ADC), RESTORE THE FOURTH, INC., AND  
NATIONAL IMMIGRATION LAW CENTER (NILC)**

The Identity Project (IDP)

<<https://PapersPlease.org>>

May 29, 2018

## I. INTRODUCTION

The undersigned civil liberties and human rights organizations – the Identity Project (IDP), Government Information Watch, Cyber Privacy Project (CPP), American-Arab Anti-Discrimination Committee (ADC), Restore the Fourth, Inc., and National Immigration Law Center (NILC) – submit these comments in response to the “60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa”, Forms DS-160 and DS-156, OMB Control Number 1405–0182, Docket Number DOS–2018-0002, FR Doc. 2018-06496, published at 82 *Federal Register* 13807-13808 (March 30, 2018), and “60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration”, Form DS-260, OMB Control Number 1405–0185, Docket Number DOS–2018-0003, FR Doc. 2018-06490, published at 83 *Federal Register* 13806-13807 (March 30, 2018).

The proposed collection of information concerning activities and identifiers on social media platforms, email addresses used, telephone numbers used, “clan”, and “tribe” does not comply with the Privacy Act, the Paperwork Reduction Act (PRA), the First and Fourth Amendments to the U.S. Constitution, or the International Covenant on Civil and Political Rights (ICCPR). This vague and overbroad collection of information from would-be visitors to the U.S. is inappropriate as a matter of policy, and contrary to U.S. national and international interests in democracy and human rights. In many cases, it would be impossible for prospective visitors to provide the requested information. Exceptions to this collection of information would be discretionary with the Department of State. The standardless and discretionary administrative decision to demand that a prospective visitor answer certain of these questions would function as a pretext for denial of admission to the U.S. that could be arbitrarily imposed against anyone.

If this proposal is submitted to OMB for approval, it should be rejected as failing to meet the statutory standard of necessity for an agency purpose and as a violation of the Constitutional and human rights of visitors to the U.S. and of U.S. citizens and residents about whom information would be collected and who want to engage in protected acts of assembly and speech with foreign visitors.

## **II. ABOUT THE COMMENTERS**

**The Identity Project (IDP)** provides advice, assistance, publicity, and legal defense to those who find their rights infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights. IDP is a program of the First Amendment Project, a nonprofit organization providing legal and educational resources dedicated to protecting and promoting First Amendment rights.

**Government Information Watch** is focused on open and accountable government. Our mission is to monitor access to information about government policy, process, and practice and to ensure and preserve open, accountable government through advocacy. In this capacity, we intend to serve as a resource for policymakers, the media, advocacy groups, and the public.

**The Cyber Privacy Project (CPP)** is a non-partisan organization focusing on governmental intrusions against Fourth and Fifth Amendment rights of privacy, particularly in government databanks and national identification schemes for voting, travel, and work, and on medical confidentiality and patient consent.

**The American-Arab Anti-Discrimination Committee (ADC)** is a nonprofit grassroots civil rights organization that seeks to preserve and defend the rights of those whose Constitutional and federal rights are violated. Founded in 1980 by U.S. Senator James Abourezk, ADC is non-sectarian and non-partisan, with members from all fifty states and chapters nationwide. ADC is dedicated to defending the Arab-American and Arab immigrant community against discrimination, racism, and stereotyping. ADC vigorously advocates for immigrant rights and civil rights for all.

**Restore the Fourth, Inc.**, is a national, non-partisan civil liberties organization dedicated to robust enforcement of the Fourth Amendment to the United States Constitution. Restore the Fourth believes that everyone is entitled to privacy in their persons, homes, papers, and effects and that modern changes in technology, governance, and law should foster the protection of this right. To advance these principles, Restore the Fourth oversees a network of local chapters, whose members include lawyers, academics, advocates, and ordinary citizens. Each chapter devises a variety of grassroots activities designed to bolster political recognition of Fourth Amendment rights. On the national level, Restore the Fourth also files amicus briefs in significant Fourth Amendment cases.

**The National Immigration Law Center (NILC)**, established in 1979, is one of the leading organizations in the U.S. exclusively dedicated to defending and advancing the rights and opportunities of low-income immigrants and their families. Our mission is grounded in the belief that every American — and aspiring American — should have the opportunity to fulfill their full potential, regardless of where they were born or how much money they have.

**III. THIS INFORMATION COLLECTION IMPLICATES FREEDOM OF MOVEMENT, FREEDOM OF ASSEMBLY, FREEDOM OF SPEECH, FREEDOM OF THE PRESS, AND FREEDOM FROM UNREASONABLE SEARCHES.**

Freedom of speech, freedom of the press, freedom of movement, freedom of association, and freedom of assembly ("the right of the people... peaceably to assemble") are recognized by the First Amendment to the U.S. Constitution. The right to be free from unreasonable searches and seizures is recognized by the Fourth Amendment.

The right to travel is also recognized in Article 12 (Freedom of Movement) of the International Covenant on Civil and Political Rights (ICCPR), a treaty ratified by, and binding on, the U.S. The ICCPR defines human rights, which by definition do not depend on citizenship.

It is a fundamental principle of statutory and Constitutional construction that whenever possible, different provisions of the Constitution and of treaties which have the same force of law should be so interpreted as to avoid inconsistency between those provisions. The only way to avoid unnecessary Constitutional conflict between the provisions of the First and Fourth Amendments and those of the parallel provisions of the ICCPR is to interpret those provisions of the Bill of Rights that are restated in the ICCPR as applying to all persons regardless of citizenship.

The Department of State, along with all other executive agencies, has been ordered by the President to consider human rights treaties including the ICCPR in performing its functions including rulemaking: Executive Order 13107, "Implementation of Human Rights Treaties," directs all executive departments and agencies to "maintain a current awareness of United States

international human rights obligations that are relevant to their functions and... perform such functions so as to respect and implement those obligations fully.”

The Department of State has reiterated in its most recent report to the United Nations Human Rights Committee that, “As reported in the Initial Report, in the United States, the right to travel – both domestically and internationally – is constitutionally protected.”<sup>1</sup> This statement was made in the context of review of U.S. implementation of the ICCPR, and in that context was clearly intended to indicate that, in the opinion of the Department of State, protection of the right to travel in the U.S. extends to all individuals regardless of citizenship.

To the extent that responding to this proposed information collection, or providing responses that the Department of State deems acceptable, is made a condition of the exercise of the right to freedom of movement, speech, and assembly, or the right to be free from unreasonable searches and arbitrary interference with privacy, it is a condition on the exercise of fundamental rights recognized in the Constitutional and international human rights treaties. Such a condition requires a showing of necessity, and is subject to strict scrutiny.

The standard for assessing whether restrictions are “necessary” and consistent with the rights recognized by the ICCPR is discussed by the U.N. Human Rights Committee in its General Comment No. 27, “Freedom of movement (Article 12)”:

[L]aws authorizing the application of restrictions should use precise criteria and may not confer unfettered discretion on those charged with their execution.... [I]t is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them. Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they

---

1 (Second and Third Periodic Reports of the U.S. Concerning the International Covenant on Civil and Political Rights, Paragraph 203, 28 November 2005, CCPR/C/USA/3, available at <[http://www.unhcr.ch/tbs/doc.nsf/898586b1dc7b4043c1256a450044f331/01e6a2b492ba27e5c12570fc003f558b/\\$FILE/G0545268.pdf](http://www.unhcr.ch/tbs/doc.nsf/898586b1dc7b4043c1256a450044f331/01e6a2b492ba27e5c12570fc003f558b/$FILE/G0545268.pdf)>, referring to Initial Report by the U.S. Concerning Its Compliance with the International Covenant on Civil and Political Rights, July 1994, CCPR/C/81/Add.4 and HRI/CORE/1/Add.49, available at <[http://dosfan.lib.uic.edu/erc/law/covenant94/Specific\\_Articles/12.html](http://dosfan.lib.uic.edu/erc/law/covenant94/Specific_Articles/12.html)>)

must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected. The principle of proportionality has to be respected not only in the law that frames the restrictions, but also by the administrative and judicial authorities in applying the law.<sup>2</sup>

Article 17 of the ICCPR provides that "No one shall be subjected to arbitrary ... interference with his privacy, family, home or correspondence." Article 19 provides, "Everyone shall have the right to ... seek, receive and impart information and ideas of all kinds, regardless of frontiers... through any ... media of his choice." Article 21 recognizes "the right of peaceful assembly" and imposes an explicit standard of necessity for restrictions on that right.

Even if U.S. accession to the ICCPR is not deemed to extend the rights recognized by the First and Fourth Amendment to all individuals regardless of citizenship, many of the individuals whose rights would be affected by this proposal are entitled to First and Fourth Amendment protection. Regarding the Fourth Amendment, the casual beliefs that the Fourth Amendment does not apply at the border or that it does not apply to non-U.S. citizens are not supported by existing Supreme Court and appeals court precedents. Just as forensic examination of a digital device at the border must be supported by reasonable suspicion of involvement in a crime (*U.S. v. Cotterman*, 2013, 9<sup>th</sup> Cir. en banc), so the seizure of an extraordinary and forensic level of detail on five years of one's travel patterns, associations, social media handles, email addresses used, and telephone numbers used, should require reasonable suspicion of involvement of the individual in a crime, rather than being a non-negotiable condition for the granting of a visa.

Many non-citizens applying for a visa are also eligible for Fourth Amendment protection of their "person, papers and effects" from "unreasonable ... seizure", as a result of meeting the test of having "substantial voluntary connections" to the U.S. (*U.S. v. Verdugo-Urquidez*, 494

---

2 CCPR/C/21/Rev.1/Add.9 (1 November 1999), available at <[http://tbinternet.ohchr.org/\\_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.9](http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.9)>

U.S. 259, 1990, plurality opinion), which test includes both U.S. persons and millions of non-U.S. persons.

In addition to the requirements of the U.S. Constitution and the ICCPR that intrusions on freedom of speech, press, movement, assembly, and privacy be justified as “necessary”, the Paperwork Reduction Act at 44 USC § 3508 imposes a specific requirement that, “Before approving a proposed collection of information, the Director [of OMB] shall determine whether the collection of information by the agency is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility.”

**IV. THIS INFORMATION COLLECTION IS NOT “NECESSARY” OR OF PRACTICAL UTILITY FOR ANY PERMISSIBLE PURPOSE, IS NOT PROPORTIONAL OR THE LEAST RESTRICTIVE INSTRUMENT FOR ACCOMPLISHING ANY PROPER AGENCY FUNCTION, AND DOES NOT WITHSTAND STRICT SCRUTINY OF ITS INTRUSIONS ON RIGHTS.**

The Department of State intends to seek OMB approval for revised versions of Forms DS-156, DS-160, and DS-260. The notices state that completion of each of these forms is “Required to Obtain or Retain a Benefit”, and each of these forms, as proposed to be revised, would require applicants for visas for admission to the U.S. to state, *inter alia*:

- “Do you belong to a clan or tribe?”
- Social media platforms and identifiers used during the last five years;
- All phone numbers used during the last five years: and



- All email addresses used during the last five years.

It should go without saying that this information, in this context, is not “necessary for the proper performance of the functions” of the Department of State.

The Department of State has been processing applications for visas for admission to the U.S. for almost two hundred years without without collecting or requiring this information. There is no indication in the notices of any circumstances in which not collecting any specific item on this list, much less all of the items on this list, would in any way prevent the Department from properly adjudicating a visa application.

A showing of necessity for collection of this information would require a showing, for each item on this list, of a situation in which that information would be relevant and potentially dispositive of some lawful, explicitly defined criterion of admissibility to the U.S. The Department of State has provided no such list.

Many of the items on this form would never be relevant to, much less dispositive of, any lawfully defined criterion of admissibility. For example, an individual cannot lawfully be discriminated against by the Department of State in adjudicating their application for admission to the U.S. on the basis of membership in, or identification or association with, a “clan” or “tribe”. “Tribe” and “clan” are not defined on the form and are not mentioned or defined in any Federal statute or regulation, except in relation to Native American tribes. But the context and the inclusion of “clan” along with “tribe” suggests that “tribe” is not being used in that sense on these forms. Depending on the community and the context, these words refer to ethnicity, race, religion, and/or national origin. Some people regard all humanity as one “tribe”.

A statute or regulation making clan or tribe a criterion for government decision-making would be void for vagueness. But it would also, by almost any definition of “clan” or “tribe”, be unconstitutionally discriminatory on its face. Any form requesting clan or tribe membership as a purported basis for government decision-making, such as the proposed Forms DS-156, DS-160, and DS-260, should be withdrawn. If submitted to OMB, it must be disapproved.

Much of the information collected on Forms DS-156, DS-160, and DS-260 pertains to U.S. persons. Children, spouses, and domestic partners of applicants for admission to the U.S. are often U.S. citizens or permanent residents. The “source of funding for travel” by individuals who are now applying for admission to the U.S. is often a U.S. person – it is routine for U.S. persons to pay for travel by friends and family visiting from less wealthy countries.

Many of those “associated” on social media with applicants for admission to the U.S. are U.S. persons. The manifest intent of the form is to collect third-party and associational data (including data about U.S. citizens) as well as first-party data. The Department of State is seeking information about social media in particular because it is *social*.

Forms DS-156, DS-160, and DS-260 do not ask applicants for visas to list their published books or articles, or the names, pen names, or pseudonyms in which they have written or published in print or electronic media other than “social media”. The notice gives no explanation of why information about publications in other media is not requested and has not been deemed “necessary” for the functioning of the Department of State, but “social media” identifiers are to be requested. The obvious inference is that, as discussed further below, the purpose of this new question on the visa is forms is to collect information not solely or primarily about applicants for visas but also about third parties, many of whom are U.S. persons.

This collection of information is not “necessary for the proper performance of the functions” of the Department of State, but has “practical utility” only for other, impermissible purposes, viz.:

- robotic predictive pre-crime profiling;
- suspicion generation and guilt by association; and
- pretextual denial of applications for visas and/or of admission to the U.S.

Consider why and how each of these invidious uses of the information collected through the proposed new questions on Forms DS-156, DS-160, and DS-260 is inevitable and is portended by the nature of this information collection:

**Robotic predictive pre-crime profiling:** The volume of information collected on the basis of the new questions on Forms DS-156, DS-160, and DS-260 is such as to preclude any possibility of it being read or individually assessed by human staff of the Department of State. Roughly 15 million individuals would be required to complete these forms each year. Consider how long it would take to review a single historical Facebook timeline, much less the snowballing web of that user's friends, people who have commented on that user's page, and people on whose pages that user has commented. It simply is not plausible to imagine that the Department of State has sufficient investigatory or visa adjudication staff to review more than a tiny fraction of even those social media postings that are in the English language. Now consider that many visa applicants' social media activities are carried on in other languages, many of them languages for which the Department of State probably has minimal staff literate and fluent in the contemporary slang used on social media. Even for the numbers of respondents estimated by the

Department of State in the notice, most of this information cannot possibly be, and will never be, read by a human being at the Department of State.

Either the Department of State wishes to amass a data lake of currently unused personal information for possible future data mining for as-yet-undefined purposes -- which would itself be unnecessary, in violation of the basic goals of the Paperwork Reduction Act, and a violation of Constitutional and international treaty privacy rights – or the Department of State wants to use this fire hose of data today as grist for the mill of robotic predictive pre-crime profiling. Or both.

This is illegitimate for two reasons. First, there is no evidence that either robotic or human "pre-cogs", or any algorithmic profiling ruleset, have any actual utility for predicting which individuals will engage in extremely rare acts of terrorism – regardless of the biographic data they are fed. Second, the Constitution does not permit the imposition of sanctions or the denial of rights based on either algorithmic scoring or predictions of possible future criminality, but only on the basis of fact-finding about past conduct proscribed by laws or regulations.

**Suspicion generation and guilt by association:** Many of the categories of information collected on Forms DS-156, DS-160, and DS-260 pertain explicitly to other individuals associated with applicants for visas or admission to the U.S. – family members, domestic partners, people who provide funds for travel – rather than to those applicants themselves. And as discussed above, other categories such as social media information and telephone numbers used implicate both applicants and their associates, but appear to have been selected for collection (in preference to otherwise similar but more narrowly targeted information, such as print publications) primarily because of their spillover into information regarding associations between visa applicants and other individuals including U.S. persons.

The notice is silent as to how information regarding clan or tribe or social media associations will be used. But any use of this associational data as the basis for decision-making would be an impermissible exercise in discrimination and/or guilt by association: placing people under suspicion and further surveillance, making adverse determinations with respect to applications for visas or admission to the U.S., blacklisting (euphemistically called "watchlisting"), or assignment of other sanctions or adverse consequences solely on the basis of familial, friendship, business, social media, clan, or tribal "associations" with other blacklisted or disfavored individuals or groups, including racial or ethnic groups.

Aside from its inherent illegitimacy as collective punishment, any such snowballing scheme of suspicion generation and guilt by association will, even if the process of linking each individual to others is nominally unbiased, tend to replicate and universalize any biases (whether with respect to religion, ethnicity, national origin, gender, political views, or otherwise) in the initial blacklist of villains or initial exemplars of negative profiles with which it is seeded.

"Garbage in, garbage out," can be restated in the context of such a suspicion-generating or guilt-by-association *deus ex machina* as, "Bigotry in, bigotry out (on an ever-growing scale)".

**Pretextual denial of applications for visas or of admission to the U.S.:** As discussed further below, many people would find it impossible to provide complete answers to the questions on Forms DS-156, DS-160, and DS-260. Because the terms used on the form are so vague, most answers could be interpreted by hostile or malign Department of State staff as inaccurate or incomplete. As with "tribe" and "clan", there is no statutory or regulatory or case law definition of "social media", for example. If an individual identifies (or is identified by others) as Jewish, are they required to state that they are a member of a clan or tribe? What if

they are descended from a member or members of an Irish or Scottish clan? What percentage of “blood” is considered determinative of membership in an ancestry-based tribe or clan? And how can the Department of State possibly think that it is permissible for a U.S. government agency to make decisions on the basis of such distinctions of race, ethnicity, creed, or national origin?

If we follow social media network connection maps as the basis for guilt by association, anyone in the world is associated with any arbitrarily designated individual or organizational "axis of evil" by no more than six degrees of separation.

One way or another, almost everyone who is asked to complete Forms DS-156, DS-160, or DS-260 will provide, either through their answers or their inability to provide them, grounds for denial of their application for a visa or for admission to the U.S., and/or for imposition of other sanctions for incomplete answers, for "false" good-faith responses to ill-defined or undefined queries, or for being "associated" (however distantly) with blacklisted individuals or organizations or groups through social media, clan, tribe, or telephone or email tree.

The risk of abuse of this information collection as a pretext for adverse action that would otherwise lack a lawful basis is greatly heightened by the lack of standards or of procedures for administrative and judicial review of decisions to require any particular individual to answer all the questions on Form DS-156, DS-160, or DS-260. The decision to require an applicant to answer all the questions on one of these forms is apparently discretionary. According to the notices, “the Department intends not to routinely ask the question [about social media] of applicants for specific visa classifications, such as most diplomatic and official visa applicants.” The use of “such as” is of course not limiting, and no criteria are specified in the notices.

Requiring an applicant to complete any of these forms with the proposed new questions can be counted on to provide some pretext for denial of the application. That means that any staff member with the authority to make that discretionary determination to order an individual to answer all the questions on Forms DS-156, DS-160, or DS-260 has the arbitrary and unreviewable power to manufacture a pretext to deny any individual's application.

**V. THIS COLLECTION OF INFORMATION UNNECESSARILY AND DISPROPORTIONATELY BURDENS FREEDOM OF SPEECH, FREEDOM OF THE PRESS, AND FREEDOM OF ASSEMBLY.**

The first and most fundamental privacy choice for a social media user (or, for that matter, for most other modes of speech and publication) is whether to write or speak in a known name, a pseudonym, or anonymously. For pseudonymous speech or writing on social media, the social media identifier or handle is effectively the "key" needed to unlock the identity of the speaker or writer, and equivalent to the password for an encrypted message.

To require a pseudonymous social media user to disclose her handle or identifier is, in effect, to require her to change her most fundamental privacy settings and to disclose the root password protecting her exercise of her rights to freedom of speech and of the press.

As such, it is *per se* an invasion of her privacy, and the legality of such a demand should be assessed according to the standards that would apply to compelled disclosure of a password.

The burden of the proposed information collection is also relevant to whether its impact on individuals and their rights is "proportional" to any utility for a permissible purpose. We

cannot overstate the significance of anonymity or pseudonymity as a potentially life-or-death matter for social media users, most especially for dissidents, victims of discrimination, and those living under the jurisdiction of repressive regimes or otherwise in fear of persecution.

Anonymous or pseudonymous speech, publication, and assembly are the only forms of dissident speech, publication, or assembly that are possible under some repressive regimes.

Activities which are protected by the First Amendment, including some which advance U.S. interests in freedom and democracy, are subject to legal sanctions in many other countries.

Capital crimes in Saudi Arabia, for example, include blasphemy against the state religion, disparagement of members of the royal family or the institution of hereditary absolute monarchy, trafficking in prohibited mind-altering substances including alcoholic beverages, and private sexual activity between consenting adults of the same gender in their home.

Saudi Arabia is a U.S. ally with which the U.S. Department of State might be expected to share information obtained through this collection of information – including information that could identify Saudi Arabian citizens or residents who have perpetrated these "crimes". As a result, this collection of information could subject these individuals, including pro-democracy activists, to sanctions in Saudi Arabia ranging from public whipping to beheading.

Even if this compelled disclosure of information were lawful – which we believe it isn't – it would be bad public policy. The possibility of anonymous and pseudonymous discourse is an essential element of an open marketplace of ideas, and plays a particularly important role in the places where identifiable speakers and speech are subject to the greatest repression.

Anonymous and pseudonymous speech and publication have a long and honorable tradition in the U.S., going back to the anonymous authors and publishers of anti-monarchist



handbills in the British colonies of North America and the pseudonymous authors of the *Federalist Papers*. Today, these works would probably be published on social media, and "Publius" – the pseudonym used by the authors of the *Federalist* – would probably be a social media "handle" rather than a name printed on the title pages of a series of pamphlets.

Anonymity and pseudonymity are especially critical for social media users, whose speech can be, and sometimes is, held not only against themselves but against any or all of their social media "friends", friends-of-friends, associates, contacts, and/or commenters.

The possibility that, at some unknown future time, any individual social media user might be required to disclose her identity to the U.S. government, and have it passed on by the U.S. to unknown third parties including other governments around the world, is already exerting a profound chilling effect on the exercise of rights to freedom of speech, freedom of the press, and freedom of assembly by individuals around the world who think they might someday wish to visit the U.S. and by U.S. citizens who wish to associate with them online and/or in person. In the absence of publicly-defined criteria for what speech on social media or association with which other individuals might lead to denial of admission to the U.S., people who want to visit the U.S. and associate with U.S. persons are afraid to say anything on social media.

**VI. THE DEPARTMENT OF STATE GROSSLY UNDERESTIMATES THE DIFFICULTY OF COMPLETING THE PROPOSED FORM AND THE TIME REQUIRED TO ATTEMPT TO DO SO.**

In the notice, the Department of State estimates that almost fifteen million individuals will be required to complete Form DS-156, DS-160, or DS-260 each year.

The notice also estimates that it will require, on average, 90 minutes for each respondent to obtain and provide the requested information. But the notice provides absolutely no basis for this estimate, and we believe that it is much too low.

Many people do not know the answers to all of the questions on Forms DS-156, DS-160, and DS-260.

The request for "Social media identifiers" is both vague and overbroad. Similar statutory mandates for persons convicted of specified sexual offenses to register with police all "social media identifiers" they use have been found to be unconstitutionally vague and overbroad.

Is a respondent expected to remember every Web site on which they have registered as a commenter, what pseudonym or handle they chose, or what auto-generated handle they were assigned? What are the chances that they will remember or reconstruct these all correctly?

Many people contribute to group blogs or to the social media profiles and message feeds of corporations, clubs, non-profit organizations, and other informal groupings. These may have multiple contributors, without contributions being individually attributed. This makes them useless for associating applicants for visas with specific statements.

The converse of the organizational social media account with multiple users is the individual with multiple social media identifiers, whether simultaneous (some people have different pseudonyms for different circles of associates) or sequential (some people are constantly forgetting their user IDs and/or passwords, and routinely sign up for one new account after another with different IDs rather than bother to try to recover their old IDs or passwords).

A public relations professional may have been one of the users of dozens or hundreds of social media accounts of her clients over the course of five years.

There are similar problems with "email addresses used during the last five years". For security or tracking or spam filtering purposes, some people use a unique "throwaway" email address each time they fill out a Web form or provide their address to a third party. They may neither remember nor keep records of most of these addresses, nor have any reason to do so.

While some people use only one email address at a time, few people use only one telephone number. We use telephones in friends' home, phones in hotels, and cellphones borrowed from strangers. Often we don't know the numbers of the phones we use, and we don't keep (and have no reason to keep) five-year logs of the numbers of every phone we have used.

We believe that 90 minutes is a gross underestimate of the time that will typically be required to complete the proposed revised Form DS-156, DS-160, or DS-260, even for those respondents who are eventually able to complete one of these forms.

Respectfully submitted,

**The Identity Project (IDP)**

<<http://PapersPlease.org>>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

\_\_\_\_\_/s/\_\_\_\_\_  
\_\_\_\_\_

Edward Hasbrouck,

Consultant to IDP on travel-related issues

**Government Information Watch**

<<http://govinfowatch.net>>

**Cyber Privacy Project (CPP)**

<<http://www.cyberprivacyproject.org>>

**American-Arab Anti-Discrimination Committee (ADC)**

<<http://www.adc.org>>

705 DeSales Street NW, Suite 500

Washington, DC 20036

**Restore The Fourth, Inc.**

<<https://www.restorethe4th.com>>

**National Immigration Law Center**

<<https://www.nilc.org>>