PRIVACY INTERNATIONAL

Privacy International's Submission to U.S. Department of State

Proposals, Submissions, and Approvals: Application for Immigrant Visa and Alien Registration

May 2018

PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

Privacy International Response to:

Agency Information Collection Activities: Proposals, Submissions, and Approvals: Application for Immigrant Visa and Alien Registration

Agency: US Department of State (DOS)

Action: Notice of request for public comment

Comments Close: 29.05.2018

ID: DOS-2018-0003-0001

Federal Register Number: 2018-06490

Docket Number: DOS-2018-0003

Information Collection title:

Title of Information Collection: Electronic Application for Immigrant Visa and Alien Registration.

OMB Control Number: 1405-0185.

Type of Request: Revision of a Currently Approved Collection.

Originating Office: Bureau of Consular Affairs, Visa Office (CA/VO/L/R).

Form Number: DS-260.

Submission via Federal e-Rulemaking Portal

And via email: *PRA_BurdenComments@state.gov*

Introduction

Privacy International wishes to raise serious concerns regarding the proposal relating to "*the Electronic Application for Immigrant Visa and Alien Registration (DS-260) which it is stated is used to collect biographical information from individuals seeking an immigrant visa. The consular officer uses the information collected to elicit information necessary to determine an applicant's eligibility for a visa.*[1]"

The Department of State is seeking Office of Management and Budget (OMB) approval for extending information collection. The intention is to revise the collection to add several new additional questions for immigrant visa applications:

> One question lists multiple **social media platforms** and requires the applicant to **provide any identifiers used by applicants for those platforms during the five years preceding the date of application.** The platforms listed may be updated by the Department by adding or removing platforms.
>
> Additional platforms will be added only if collection is consistent with the uses described in the Supporting Statement and after Office of Management and Budget approval.
>
> In addition, the applicant will be given the option to **provide information about any social media identifiers associated with any platforms other than those that are listed that the applicant has used in the last five years**.
>
> The Department will collect this information for identity resolution and vetting purposes based on statutory visa eligibility standards.
>
> Other questions seek **five years of previously used telephone numbers**, **email addresses**, and **international travel**; all prior immigration violations; and whether specified family members have been involved in terrorist activities.

The Supporting Statement states that the new required question labelled 'Social Media' will instruct:

> "Select from the list below **each social media platform you have used within the last five years**. In the space next to the platform's name, **enter the username or handle you have used on that platform**. If you have used more than one platform or more than one username or handle on a single platform, click the "Add Another" button to list each one separately. If you have not used any of the listed social media platforms in the last five years, select "None."
>
> The form will include a data field labelled "Social Media Identifier" for the applicant to type in his or her **social media "handle" or identifier.** The applicant may select "Add Another" if the applicant

[1] https://www.regulations.gov/document?D=DOS-2018-0003-0001

has more than one provider/platform or social media identifier to disclose. Applicants will be advised they do not need to list accounts designated for multiple users within a business or other organization. Applicants may be provided help boxes to assist in common questions, such as how to find the "social media identifier" of an account. Applicants will be advised to list each identifier used, including multiple identifiers on a single platform. No visa application is guaranteed approval, and all can be denied for a variety of reasons, but an applicant who does not have a social media presence will not be denied on that basis.

The platforms listed may be updated by the Department by adding or removing platforms. Additional platforms will be added only if collection is consistent with the uses described in the Supporting Statement and after Office of Management and Budget approval.

In addition, a new optional question on the DS-160 and DS-156 will ask applicants **if they wish to provide any other social media identifiers for platforms they have used within the last five years to create or share content (photos, videos, status updates, etc.) not listed in the initial social media question**. The question will require applicants to respond "yes" or "no," but applicants who decline will not be required to provide any additional identifiers.

The Department will collect this information for identity resolution and vetting purposes based on statutory visa eligibility standards.

….

f. Applicants are currently asked for their current email address. Applicants will be asked "Have you used any other **email addresses** during the last five years?" An affirmative response will permit applicants to add additional addresses used.

[emphasis added]

The Department seeks to:

- Evaluate whether the proposed information collection is necessary for the proper functions of the Department.
- Evaluate the accuracy of our estimate of the time and cost burden for this proposed collection, including the validity of the methodology and assumptions used.
- Enhance the quality, utility, and clarity of the information to be collected.
- Minimize the reporting burden on those who are to respond, including the use of automated collection techniques or other forms of information technology.

In summary, we believe that:

- The proposed information collection is not necessary for the proper functions of the Department.

We understand that questions about social media identifiers were added to the applications for visas and ESTA forms in 2016 but until now the State Department claimed that answering these questions was voluntary.

We note that in October 2017, the Department of Homeland Security published the 'notice of modified Privacy Act System of Records'[2] to which we responded.

We are disappointed that despite serious concerns raised in relation to the previous publication, the Department of Homeland Security now seeks to expand similar policies designed to monitor social media and surveil email and telephones via data collection. We understand that previously there were not requirements for would-be visitors or immigrants to the US to provide current or past telephone numbers, e-mail addresses or a comprehensive list of which countries other than the US have been visited or when they have been visited. This is now required. In addition, as noted above, social media identifiers are sought for a period of five years.

The desire to expand the use of social media intelligence without sufficient justification that this is necessary and proportionate represents a gross intrusion into individual's right to privacy. At the very least it will cause both immigrants and citizens in the US, together with the millions who interact online, to mistrust social media and cause unease in relation to their online activities. At worse it will have a chilling effect on free speech of all internet users who openly express personal or political views in case such rules could someday apply to them. It erodes the right to private life and personal autonomy whilst expanding unchecked mass surveillance.

For a number of years, the DHS has been collecting and scrutinizing the social media of certain immigrants and foreign visitors. This is part of a larger process of high-tech surveillance of immigration and desire to subject more and more people to social media screening.

The desire to collect and exploit social media via the gathering of social media handles and conduct social media monitoring will have wide-reaching negative impacts and we call for an urgent review of all collection, retention and processing activities not only in relation to this proposal but more broadly throughout government.

Any use of SOCMINT must comply with the international principles of legality, necessity and proportionality.

---

[2] Agency: Department of Homeland Security, Privacy Office
Action: Notice of Modified Privacy Act System of Records
Comments Close: 18.10.2017
Document Citation: 82 FR 43556
Agency / Docket Number: DHS-2017-0038
Document Number: 2017 – 19365

Summary background

The Supporting Statement refers to the Immigration and Nationality Act 8 U.S.C which provides that applicants for visas must provide 'additional information necessary to the identification of the application and the enforcement of the immigration and nationality laws as may be by regulations prescribed.'

The Supporting Statement goes on to refer to Executive Order 13780 in relation to 'screening and vetting procedures' and cites the Memorandum of the Secretary of State, the Attorney General and the Secretary of Homeland Security, issued March 6, 2017, in which the President stated:

"[t]o avert the entry into the United States of foreign nationals who may aid, support, or commit violent, criminal or terrorist acts, it is critical that the executive branch enhance the screening and vetting protocols and procedures for granting visas, admission to the United States, or other benefits under the INA."

In this light, the purpose of the information gathering is to 'enable consular officers to adjudicate visa eligibility requirements'.

The Supporting Statement estimates that 710,000 applicants annually will complete this collection.

Highly invasive

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 and interacting online.

To permit the collection of 'social media handles, aliases, associated identifiable information' to enable monitoring of social media platforms and to expand sources to 'publicly available information obtained from the internet' is to give a deep understanding of our social interactions, our habits, our location and our daily lives. Social media intelligence ("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'.

The use of ("SOCMINT"), the techniques and technologies used to monitor social media networking sites such as Twitter and Facebook, represents a significant intrusion into individual privacy. "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. In May 2017 Facebook told advertisers it can identify emotions such as teenagers feeling "insecure and

worthless".[3]

Wide impact

The proposals represent a grave intrusion into the private lives of potentially hundreds of thousands of individuals. 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, can you anticipate 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.

The data that will be collected is highly invasive and the scale and scope of the program would lead to a significant expansion of intelligence activity.

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 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."[4]

- 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.[5]

- 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".[6]

Automated decision making

Previous proposals and the February 2017 Report have indicated that the methods of analysing social media networking sites vary and include manual and automated review. The current 'Agency Information Collection Activities:

---

[3] https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens
[4] https://www.privacyinternational.org/node/1481
[5] https://www.privacyinternational.org/node/1481 & https://www.privacyinternational.org/node/935
[6] https://www.reprieve.org.uk/press/saudi-government-threatens-death-penalty-for-tweeting-reports/

Proposals, Submissions, and Approvals: Application for Immigrant Visa and Alien Registration' does not specify what tools will be used.

Thus, we lack clarity in relation to how social media identifiers will be used to gather information on individuals, what queries will be run and how this is used to grant or reject a visa application. We are concerned at the lack of transparency in respect of the use of manual and automated collection techniques. 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"*[7]

Unintended consequences and abuse

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.

Clarification is required

The vague nature of this proposal and lack of elaboration is a serious cause for concern, particularly for all wishing to travel to the US for family, business and personal reasons. We note a few key unanswered matters:

1. No definition is provided for "social media platforms" and "handles" nor sufficient information as to whether for example this includes work, personal or other group based social media activity;

2. There is no detail on how this process will operate.

---

[7] 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)

3. No explanation is provided why and how this information is necessary and proportionate to the intended purpose;

4. It was unclear whether the monitoring would take place and when. Would searches also be conducted on disclosed social media handles after application process.

5. There is no indication what procedures are in place for oversight, safeguards, safe storage and deletion of data.

6. There is no indication that individuals will be able to obtain full copies of their files, including electronic sources, to ensure that data held about them is accurate and up to date.

We note the in February 2017**,** the Officer of Inspector General reported on 'DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success' found that[8]:

> 'these pilots, on which DHS plans to base future department-wide use of social media screening, **lack criteria for measuring performance to ensure they meet their objectives.** Although the pilots include some objectives, such as determining the effectiveness of an automated search tool and assessing data collection and dissemination procedures, it is not clear DHS is measuring and evaluating the pilots' results to determine how well they are performing. Absent measurement criteria, the pilots will be of limited use in planning and implementing an effective, department-wide future social media screening program.'

As noted above, there is lack of detail regarding how the proposal will be implemented and what will be swept up in the authorities collection. The February 2017 report states noted the US authorities have been trialling the use of automated tools:

> *'social media analytics tool, covers a large number of social media platforms, has access to third-party information providers, and can access web-based information.'*

In relation to the April 2017 pilot the report states:

> *In reviewing the pilot, USCIS concluded that the tool was not a viable option for automated social media screening and that manual review was more effective at identifying accounts. USCIS based its conclusion on the xxxx tool's low "match confidence." Because the resulting accounts identified by the tool did not always match up with the applicants, officers had to manually check the results. However, USCIS did not establish match benchmarks for the tool, so it does not know what level of match confidence would signify success or failure.*

---

[8] https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf

Conclusion

Numerous and important questions remain outstanding and urgently need to be publicly clarified. From the Supporting Statement it is clear there is in sufficient justification to establish that this is effective, necessary and proportionate, and as such is an unlawful invasion into privacy.

Social media, which can include a wide range of online platforms and applications, can be revealing and sensitive, making any collection or retention highly invasive. The effect would be unjustified intrusion into the private lives of those affected, undermining their freedom of speech and affecting everyone in their networks, including US citizens.

By normalising the practice internationally, other state authorities may reciprocate by demanding social media handles of US citizens, undermining their rights as well as their security while travelling.

The potential use of automated decision-making, including through the use of profiling, poses significant rights, since derived, inferred or predicted profiles may be inaccurate, or otherwise systematically biased, leading to individuals being wrongly denied a visa.

We call for an urgent review of all collection, retention and processing activities, not only in relation to this proposal but more broadly of the use of social media intelligence and open source intelligence, throughout DHS and other government departments.

About Privacy International

Privacy International (PI) is a registered charity based in London that works at the intersection of modern technologies and rights.

We shine a light on overreaching state and corporate surveillance, with a focus on the sophisticated technologies and weak laws that enable serious incursions into our privacy. We investigate, litigate, advocate and educate, all with one aim - for people everywhere to have greater security and freedom through greater personal privacy.

We work with experts all over the world to build the global privacy movement.