Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and the Special Rapporteur on the right to privacy

REFERENCE:
OL USA 9/2018

18 May 2018

Excellency,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and Special Rapporteur on the right to privacy, pursuant to Human Rights Council resolutions 34/18 and 37/2.

In this connection, we would like to bring to the attention of the U.S. Government information we have received concerning the Department of State's proposal to require travelers' social media information on various United States' immigration forms. Concerns about intensified social media screening at the border were raised in a previous communication sent on 1 May 2017 (USA 7/2017), and concerns about amendments to the Electronic System for Travel Authorization (ESTA) requesting information of travelers' social media were raised on 30 September 2016 (USA 9/2016). The latter concerns were also discussed with representatives of your Government on 14 October 2016, via conference call. We acknowledge your response dated 14 September 2017 to the communication sent on 1 May 2017(USA 7/2017), but remain concerned in light of the new information received:

> The Department of State intends to expand its social media collection program through its proposed changes to Form DS-260, the Electronic Application for Immigrant Visa and Alien Registration, and Forms DS-160/DS-156, the online and written Applications for Nonimmigrant Visas.
>
> The changes will require visa applicants to provide any identifiers used by applicants for multiple social media platforms listed in the revised forms. It is unclear which platforms will be listed.
>
> Applicants will be required to specify identifiers used on those platforms "during the five years preceding the date of the application."
>
> The Department of State has the discretion to add or remove listed platforms.
>
> Applicants will also be given the option to provide information about any social media identifiers associated with any platforms other than those that are listed and that the applicant has used in the last five years.
>
> Additionally, the revised forms will "seek" information concerning "five years of previously used telephone numbers, email addresses, and international travel."

The Department of State claims that the proposed collection of information will bring forth "information necessary to determine an applicant's eligibility for a visa" and estimates this new program will affect at least 710,000 immigrant visa applicants and 14 million non-immigrant visa applicants.

Before identifying concerns raised by the proposal, we wish to reiterate that Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which the United States ratified on 8 June 1992, protects everyone's right to maintain an opinion without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. Under article 19(3) of the ICCPR, restrictions on the right to freedom of expression must be "provided by law," and necessary for "respect of the rights or reputations of others" or "for the protection of national security or of public order, or of public health and morals." Permissible restrictions on the Internet are the same as those offline (A/HRC/17/27).

In addition, article 17(1) of the ICCPR provides for the rights of individuals to be protected, inter alia, against arbitrary or unlawful interference with their privacy and correspondence, and provides that everyone has the right to the protection of the law against such interference. Articles 17 and 19 of the ICCPR are closely connected, as the right to privacy is often understood to be an essential requirement for the realization of the right to freedom of expression (A/RES/68/167, A/HRC/27/37, A/HRC/23/40, A/HRC/29/32).

Under the article 19(3) requirement of legality, it is not enough that restrictions on freedom of expression are formally enacted as domestic laws and regulations. Instead, restrictions must also be sufficiently clear, accessible and predictable (CCPR/C/GC/34). While surveillance measures and other restrictions on freedom of expression may be established to protect national security and public order, they must be "necessary" to protect such objectives, and not simply useful, reasonable or desirable. The requirement of necessity "also implies an assessment of the proportionality" of those restrictions. A proportionality assessment ensures that restrictions "target a specific objective and [do] not unduly intrude upon other rights of targeted persons." The ensuing "interference with third parties' rights must [also] be limited and justified in the light of the interest supported by the intrusion" (A/HRC/29/32). Finally, the restriction must be "the least intrusive instrument among those which might achieve the desired result" (CCPR/C/GC/34).

Based on the United States Government's obligations under the ICCPR, we are concerned about the proposal on several grounds, many of which mirror the concerns raised in 2016 and 2017:

Scope of information collected

Through its proposed collection, the government could potentially collect, based on disclosed identifiers, five years' worth of personal and sensitive information such as one's social, religious and political views and opinions, pictures, contact lists and

geolocation information. Such information could be collected about not only applicants who must provide these identifiers, but also their family members, colleagues and other contacts in their social and professional online networks.

Additionally, the proposed collection will also encompass "five years of previously used telephone numbers, email addresses, and international travel." The proposal is silent on whether these disclosures are voluntary, and how they will aid the vetting process. This ambiguity, combined with the prospect of ineligibility, might lead individual travelers to feel obliged to provide information even if the question is characterized as optional. Furthermore, such information could be analyzed in tandem with information collected from social media to create an intimate and detailed mosaic of the applicant's movements, associations, and personal and professional lives.

Finally, the proposed "option to provide information about any social media identifiers associated with any platforms other than those that are listed" is also unclear about how incomplete responses or leaving it blank will affect an individual's application (for example, whether it will result in additional screening procedures or alternative forms of scrutiny). It also does not provide information about the kinds of platforms the government deems relevant to include, and could potentially encompass a wide range of platforms from gaming, dating, ride sharing and shopping (to name a few).

Use of information

The proposal is unclear about how collection of this information will aid the Department in "identity resolution and vetting purposes" and in determining "the applicant's eligibility for a visa." The proposal also does not address how ambiguity in the meaning and significance of social media information—such as a user's intention when she clicks the "like" button on a Facebook post or retweets a tweet or link on Twitter—will be taken into account during the vetting process. As a result, individuals may fear that their activities on social media platforms will be misconstrued, and used against them; this fear can even lead individuals to delete their profiles on such platforms entirely. Additionally, the Department has not addressed how social media information of contacts associated with applicants may be utilized in the process.

Discretion and authority of consular officers

The proposal does not provide guidance on the follow-up action(s) that consular officers are permitted or required to take when they receive social media information. For example, it is unstated whether (and under what circumstances) officers may request additional information or access to private accounts, such as through passwords. It is also unclear whether officers can request or persuade travelers who have left optional data fields blank to provide information, or whether they would be questioned as to why they left the field blank, or whether they will contact family members and contacts of the applicants.

Other uses of information collected

The proposal is silent on whether the information collected will be used for purposes other than vetting or assessing a traveler's visa eligibility. For example, it is unstated whether such information could be used to assess the traveler's eligibility for other visas, or other government benefits or privileges. It is also unclear how the Department will share the information collected with other government agencies, such as law enforcement and intelligence authorities, or even other foreign governments.

No timeline has been provided for how long such information may be stored nor any information about where it will be stored.

These concerns implicate the government's obligation to ensure that restrictions on freedom of expression are "provided by law" in accordance with Article 19(3) of the ICCPR. In particular, we are concerned that visa applicants have insufficient guidance on what information may be collected about them through their social media accounts, and how such information may be analyzed and assessed for both visa application and other purposes. For data fields that are optional, we are concerned that applicants lack sufficient guidance on what information to provide, and the consequences of not providing it.

These concerns also implicate the requirement that restrictions on freedom of expression must be necessary and proportionate in accordance with Article 19(3). The government already collects a wide range of information about visa applicants to assess their eligibility; it is unclear how information collected about the applicant's social media activities will enhance these assessments. In fact, the highly subjective and conclusory nature of social media information (e.g. a retweet of a controversial opinion may be incorrectly deemed an endorsement of that opinion) may hamper the accuracy and timeliness of such assessments.

The proposal's lack of clear and meaningful limits concerning the scope of information collected and how it will be used also imbues the government with expansive authority to conduct intrusive surveillance on visa applicants and their associations. Awareness that multiple government agencies will have access to such personal and sensitive information – and uncertainty about how the government will interpret and use it – may incentivize self-imposed restrictions on the applicant's online activities and other forms of self-censorship. Fear that one's online activities may lead to an adverse outcome or denial of entry is likely to exacerbate these chilling effects. These effects may be even more pronounced with applicants in highly visible occupations or from communities at-risk, such as journalists, activists, artists and academics. We are concerned that these interferences with freedom of expression are disproportionate to any additional protection social media data collection and analysis might provide, particularly in light of questions about the legitimacy and usefulness of such data.

It is our responsibility under the mandates provided to us by the Human Rights Council to clarify all cases brought to my attention. Therefore, we would welcome any

additional information or clarification from the U.S. Government with respect to the proposal and on measures taken to ensure that it complies with the United States' obligations under international human rights law, particularly with respect to the right to freedom of opinion and expression. We would also welcome the opportunity to discuss the proposal in more detail with Government officials at their convenience.

Finally, we would like to inform your Government that this joint communication will be made available to the public and posted on the website page for the mandate of the Special Rapporteur on the right to freedom of expression: (http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/LegislationAndPolicy.aspx).

Your Government's response will also be made available on the same website as well as in the regular periodic Communications Report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of our highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Joseph Cannataci
Special Rapporteur on the right to privacy