

Comments of the Center for Democracy & Technology

Re: Agency Information Collection Activities: Electronic Visa Update System

24 April 2017

The Center for Democracy & Technology writes to convey our concerns with the U.S. Department of Homeland Security (DHS) proposal—to be implemented through U.S. Customs and Border Protection—to ask Chinese recipients of the B-1, B-2, and combination B-1/B-2 visas to provide their social media identifiers on the Electronic Visa Update System (EVUS) form.¹ DHS proposes to ask Chinese visitors completing the EVUS to provide “information associated with [their] online presence,” including the “provider/platform” and “social media identifier” used by the applicant.² These appear to be the same prompts that DHS recently added to the Electronic System for Travel Authorization (ESTA) application for the Visa Waiver Program (VWP).³

As we commented in response to the Federal Register notice proposing the change to the VWP application,⁴ CDT is deeply concerned that this proposal would invade the privacy and chill the freedom of expression of visitors to the United States and United States citizens.

In our prior comments on the VWP proposal, CDT noted: (1) The invasiveness of online identifier collection; (2) overbroad expansion of intelligence activity; (3) disproportionate risks of online identifier collection; (4) the ineffectiveness of online identifier collection in screening visa applicants; and (5) the costliness of this collection and analysis.⁵

These same concerns persist with the current proposal to expand the EVUS to collect online identifiers and we include those comments below. Collection and review of individuals’ social media activity will invade the individual privacy of Chinese citizens and the U.S. citizens that are their social media contacts. This significant increase in data collection will undoubtedly create chilling effects on their communications. It is not likely to yield useful information to prevent terrorist attacks and will create substantial additional costs for DHS with little apparent benefit.

¹ U.S. Customs & Border Protection, Agency Information Collection Activities: Electronic Visa Update System, FederalRegister.gov (Feb. 21, 2017), <https://www.federalregister.gov/documents/2017/02/21/2017-03343/agency-information-collection-activities-electronic-visa-update-system>.

² *Id.*

³ See Edward Helmore, “US government collecting social media information from foreign travelers”, the Guardian (Dec. 26, 2016), <https://www.theguardian.com/world/2016/dec/26/us-customs-social-media-foreign-travelers>.

⁴ Comments to DHS on Proposal to Ask Visa Waiver Applicants for Social Media Identifiers, Center for Democracy and Technology (Aug. 22, 2016), <https://cdt.org/files/2016/08/CDT-comments-DHS-social-media-identifier-proposal.pdf>.

⁵ Coalition Letter Opposing DHS Social Media Collection Proposal, Center for Democracy and Technology (Aug. 22, 2016), <https://cdt.org/files/2016/08/DHS-SM-Coalition-letter-updated-signatory-list.pdf>.

Moreover, due to the Chinese government's extensive censorship and surveillance of online activity in China (see Section IV below), requesting Chinese visitors to disclose their online activity may have a particularly strong chilling effect. Depending on which websites and online services are listed on the EVUS form, the question may prompt Chinese citizens to identify social media activity that may be prohibited in China (but which could be wholly lawful within the United States). The extent to which DHS may share this information with foreign governments will not be clear to Chinese citizens as they complete the form, which could further encourage Chinese travelers to self-censor their online activity or to omit information from the EVUS.

For all of these reasons, we urge DHS to withdraw this proposal and to reject any approach that involves suspicionless monitoring and review of individuals' social media activity.

I. Online identifier collection is highly invasive.

DHS proposes to request that individuals completing the EVUS form provide "information associated with [their] online presence" including "provider/platform" and "social media identifier." Unlike a request for an individual's address or phone number, which is a distinct question that yields a specific, static data point, a request for information about an individual's online presence is an open-ended inquiry that seeks to enable CBP to review historical, ongoing, and prospective communications activity. The DHS proposal would ask travelers to give CBP a window into many of their online activities. Indeed, travelers may not be fully aware of the amount of information that they are disclosing or the scope of CBP's review of their online activity.

Due to the lack of clear definition of "platform" and "social media identifier", individuals may feel compelled to provide information about their use of dating services, online review sites, classified ads sites, or other types of public online "platforms" that enable individuals to communicate with one another. In general, Chinese travelers will face significant incentive to provide information about their online activity, rather than risk being denied a visa or admission into the U.S. Even though the prompt would be marked "optional", cautious travelers are likely to over-provide information if they are concerned that a failure to do so will result in an adverse decision.

II. Collection of online identifiers creates a significant burden on the freedom of expression of Chinese citizens.

The risk of an adverse decision by CBP officials is also likely to drive a significant chilling effect on the freedom of expression of Chinese travelers to the U.S. The communications and information that individuals post on their public social media accounts are highly contextual and vulnerable to

interpretive error. Error is particularly likely when the interpreter does not speak the language or lacks cultural, colloquial, or idiosyncratic touchstones necessary to understand the collected content.⁶

It is unclear what type of online activity would merit the denial of a visa or admission to the U.S, according to CBP officials. For example, it is not clear whether information posted by third parties (“friends” or “followers”) on a person’s social media feeds will be considered relevant to the determination of admissibility. This is particularly problematic because there is no clear point in the review process when applicants given an opportunity to provide an explanation to explain information associated with their online profiles or challenge a potentially inappropriate denial of a visa waiver. As a result, Chinese travelers will feel pressured to curate their online accounts so that they do not reflect potentially controversial or sensitive information.

III. The proposed data collection will be ineffective and will impose significant costs.

The ease with which travelers with ill intent can edit, remove, or fabricate public social media postings also means it is highly likely that most of the information disclosed on EVUS will be useless to DHS. Individuals who pose a threat to the United States are highly unlikely to volunteer online identifiers tied to information that would hinder their admissibility to the United States. The more likely result is that DHS will be inundated with information from innocent travelers who feel compelled to disclose information to limit the risk of an adverse admissibility decision. Moreover, the cost associated with and meaningful sorting and analysis of the flood of information that is broadly related to an individual’s “online presence” would add a tremendous cost and administrative burden.

IV. The potential chilling effect on online activity of DHS requests for social media identifiers is heightened in the Chinese context.

Chinese citizens already face significant censorship and surveillance in their home country. In 2016, Freedom House identified China as “the world’s worst abuser of internet freedom” for the second consecutive year.⁷ The Chinese government routinely censors communications on social media and blocks entire websites and platforms from access within the country.⁸

The Federal Register notice does not specify which online services or platforms DHS plans to include on the EVUS form. On the current version of the Electronic System for Travel Authorization form, VWP applicants are prompted to provide their identifiers on thirteen different platforms: AskFM, Facebook, Flickr, GitHub, Google+, Instagram, JustPaste.it, LinkedIn, Tumblr, Twitter, Vine, VKontakte, and

⁶ This type of interpretive error has occurred previously. See, e.g., Caution on Twitter urged as tourists barred from US, BBC.com (Mar. 8, 2012), <http://www.bbc.com/news/technology-16810312>.

⁷ Freedom House, Freedom on the Net 2016, China Report 2, <https://freedomhouse.org/sites/default/files/FOTN%202016%20China.pdf>.

⁸ *Id.* at 7-10.



YouTube. Of these thirteen platforms, at least eight appear to currently be blocked from access in China.⁹

Chinese citizens may have accounts on these blocked platforms through any number of means, including creating and accessing accounts while outside of China or accessing the blocked sites using circumvention technology. However they may come to access these popular sites, Chinese citizens may balk at a request from a government official to disclose their use of these platforms, and either provide inaccurate information or no information at all (limiting any utility of this information collection for CBP). Conversely, many Chinese citizens may not have accounts on the platforms included on the EVUS form and may worry that their failure to provide information will negatively affect their ability to enter the U.S.

China has also increasingly pushed for real-name registration on popular Chinese sites.¹⁰ If a Chinese citizen operates under a pseudonym on one of the platforms listed on the EVUS, they may risk disclosing activity that is prohibited by the Chinese government and linking their offline identity to this online activity. Concerns about breach of CBP records and the potential for information-sharing among governments are thus heightened for Chinese travelers. The potential chilling effect, particularly on those journalists, advocates, and others who would voice disagreement with the Chinese government, is likewise even stronger in the EVUS context.

* * *

DHS's proposal to collect the online identifiers of travelers will burden fundamental rights, is likely to be both expensive and ineffective, and poses a particularly strong threat of chilling the freedom of expression of Chinese citizens seeking to travel to the U.S.

Furthermore, if DHS continues to expand its requests for information concerning travelers' online activity, this will inevitably lead to other countries making the same demands of U.S. citizens who seek to travel abroad—and providing accurate information about one's online activity may not be voluntary, under these other regimes. We urge DHS to withdraw the proposal.

Respectfully submitted,
Emma Llansó
Taylor Moore

Center for Democracy & Technology

⁹ GreatFire.org reports that Facebook, Flickr, GitHub, Google+, Instagram, Tumblr, Twitter, and YouTube are currently blocked in China. GreatFire.org, *Censorship of Alexa Top 1000 Domains in China*, <https://en.greatfire.org/search/alexa-top-1000-domains> (last accessed 24 April 2017).

¹⁰ See, e.g., Josh Chin, *China Is Requiring People to Register Real Names for Some Internet Services*, *The Wall Street Journal* (Feb. 4, 2015), <https://www.wsj.com/articles/china-to-enforce-real-name-registration-for-internet-users-1423033973>.