CENTER FOR DEMOCRACY & TECHNOLOGY

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 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.

CENTER FOR DEMOCRACY & TECHNOLOGY

Comments of the Center for Democracy & Technology

Regarding Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization

19 August 2016

The Center for Democracy & Technology appreciates the opportunity to provide comments to the Department of Homeland Security on its proposal to begin requesting disclosure of social media identifiers and other online account information from Visa Waiver Program applicants. DHS proposes to ask foreign visitors applying for a waiver of visa requirements to provide "information associated with [their] online presence," including the "provider/platform" and "social media identifier" used by the applicant. While the details of this proposed information collection are unclear, DHS's Notice of Collection Activities states that the solicited online identity information "will enhance the existing investigative process" and "provide DHS greater clarity and visibility to possible nefarious activity and connections" of visitors to the United States.[1]

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.

Under the proposed changes, visitors to the U.S. who seek admittance through the Electronic System of Travel Authorization (ESTA), or complete Form I-94W, will be subject to unspecified review and monitoring of their public online activity by U.S. Customs and Border Protection (CBP) officials. This program will also increase the surveillance of U.S. citizens, both as a result of their online connections to visitors to the U.S. and because other countries may seek similar information from U.S. citizens traveling abroad. The burdens of this scrutiny will undoubtedly fall disproportionately on visitors and U.S. citizens who are Muslim or who have connections to the Middle East.

In addition to these challenges for fundamental rights, the proposal has a number of practical drawbacks as well. First, it is unlikely to yield useful information for CBP officials. Bad actors could easily circumvent the request by providing intentionally false or incomplete information. Further, the expense of the proposed data collection and analysis is significantly underestimated in the Request for Comment. In-depth, unbiased evaluation of a prospective visitor's public social media posts and connections cannot be accomplished in an automated fashion and would require extensive—and costly—human review.

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.

---

[1] U.S. Customs & Border Protection, Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization, FederalRegister.gov (June 23, 2016), https://www.federalregister.gov/articles/2016/06/23/2016-14848/agency-information-collection-activities-arrival-and-departure-record-forms-i-94-and-i-94w-and (hereinafter "Federal Register Notice").

CENTER FOR DEMOCRACY & TECHNOLOGY

I. Requesting disclosure of online identifiers in the Customs process would create a significant burden on the free expression and privacy of international travelers.

The proposed information collection would affect visitors who are traveling with a passport issued by one of the Visa Waiver Program designated countries, including Japan, South Korea, Singapore, Chile, Taiwan, and many members of the European Union and other European countries.[2] If arriving by air or sea, these travelers must fill out an ESTA form at least 3 days before their intended arrival to the U.S. and renew it at least every two years. In 2014, over 22 million visitors entered the U.S. through the Visa Waiver Program.[3] In addition to tourists, this includes family members, patients, amateur athletes and musicians, scholars, conference attendees, business visitors, and entrepreneurs.[4]

The scope of these visitors' online activity is enormous, and the proposal provides no definition of "online presence", "provider/platform", or "social media identifier" to narrow the field. This creates the potential for an overly broad or arbitrary interpretation by CBP officials or applicants who are concerned about being denied a visa waiver. Millions of websites and online services allow, and sometimes require, users to create a username or other identifier to post content and connect with other users. In the realm of travel-related services alone there are dozens of sites and apps that might fit the bill, including TripAdvisor, Yelp, AirBnB, VRBO, Couchsurfing, Hostelworld, Uber, Lyft, Tripatini, Google+ (including Google Maps and Translate), Foursquare, and WikiTravel. Or DHS may be focused on more general-purpose services such as Facebook, Twitter, YouTube, SnapChat, Instagram, Pinterest, Tumblr, Reddit, LiveJournal, XING, StudiVZ, Hyves, Fotolog, KakaoTalk, LINE, WeChat, Pixnet, Xuite, Plurk, or even dating services such as Tinder, Grindr, and OKCupid. Any of these, and thousands more, could represent a portion of an individual's "online presence". DHS has provided no explanation of what type of response it expects from visitors.

While the Request for Comments describes the request for applicants' social media identifiers as "an optional data field," applicants for a visa-waiver will likely feel compelled to disclose significant amounts of personal information in response to this question. The majority of the data fields on the ESTA form are mandatory, and absent a specific indication to the contrary, it is likely that applicants will presume this question is mandatory as well.

---

[2] A full list of Visa Waiver Program designated countries is available at 8 C.F.R. § 217.2.
[3] 2014 Yearbook of Immigration Statistics, *available at* https://www.dhs.gov/sites/default/files/publications/table28d_7.xls. In 2010, Visa Waiver Program visitors contributed over $60 billion in tourism revenue. The White House, Office of the Press Secretary, Obama Administration Continues Efforts to Increase Travel and Tourism in the United States (May 10, 2012), *available at* https://www.whitehouse.gov/the-press-office/2012/05/10/obama-administration-continues-efforts-increase-travel-and-tourism-unite. The U.S. Travel Association estimates that, in 2015, Visa Waiver Program visitors "generated $120 billion in total output for the U.S. economy, supporting nearly 800,000 American jobs." U.S. Travel Association, Visa Waiver Program, *available* at https://www.ustravel.org/issues/visa-waiver-program.
[4] U.S. Department of State, Bureau of Consular Affairs, Visa Waiver Program, *available at* https://travel.state.gov/content/visas/en/visit/visa-waiver-program.html.

Even if this question is clearly marked "optional", however, most applicants will likely feel substantial pressure to provide some information in response, because it is unclear whether refusing to provide this information could result in CBP officials drawing adverse inferences. The consequences of a visa-waiver denial to the visitor, her family, her business associates, and her fellow travelers can be significant. Travelers are able to fill out an ESTA application online at their convenience. The form takes an average of 20 minutes and there is a $14 fee per application.[5] In contrast, visa applications require the applicant to visit a consulate in person and can take months to process.[6] Assuming the traveler has enough time to apply for a visa after being denied a waiver, the B1 visa costs at least $160, plus any expenses incurred traveling to a consulate to apply in person.[7] As a result, if a traveler's ESTA application is rejected, that traveler could be prevented from coming to the U.S. entirely. This creates a considerable incentive to respond thoroughly to every question asked in the waiver-request process.

Potential visitors to the U.S. will thus be faced with a choice between two undesirable options: decline to disclose information about their online identity and risk being denied a waiver for providing incomplete information, or disclose this information and risk denial due to inaccurate or prejudicial inferences made about their online activity. It is unclear what sort of online activity CBP officials would consider to merit denial of a visa waiver; as we discuss below, evaluation of public social media posts and connections for accurate, actionable intelligence is an extremely complex task. As a practical matter, applicants would have little or no opportunity to explain information associated with their online profiles or challenge inappropriate denial of a visa waiver. And, while denial of a person's visa-waiver request does not preclude their entry to the U.S. by a standard visa, most travelers would reasonably assume that an adverse decision on their ESTA application would translate to a similarly adverse decision on the issuance of a visa.

Thus, this proposal will create a chilling effect for travelers wishing to come to the U.S.[8] The risk of denial based on their online presence could lead some visa-waiver applicants to delete sensitive or controversial accounts in preparation for travel to the U.S., or simply to forgo an online presence at all. The strong incentives to disclose, and the unknown risks of nondisclosure, will compel many other applicants to share abundant information about their online activity. Most of these innocent disclosures will be useless for screening purposes, but they may still be used to augment the growing intelligence surveillance apparatus—with little legal protection for personal information and few, if any, mechanisms to safeguard against abuse.

---

[5] Department of Homeland Security, Official ESTA Application, https://esta.cbp.dhs.gov/esta/.
[6] Visas can take months to process. U.S. Customs & Border Protection, Frequently Asked Questions about the Visa Waiver Program (VWP) and the Electronic System for Travel Authorization (ESTA), https://www.cbp.gov/travel/international-visitors/frequently-asked-questions-about-visa-waiver-program-vwp-and-electronic-system-travel.
[7] U.S. Bureau of Consular Affairs, Visitor Visa, https://travel.state.gov/content/visas/en/visit/visitor.html#fees.
[8] *See, e.g.*, Caution on Twitter urged as tourists barred from US, BBC.com (Mar. 8, 2012), http://www.bbc.com/news/technology-16810312.

II. The proposed collection is highly invasive and offers no assurances against abuse.

Currently, the visa-waiver application solicits information about a prospective visitor's name, address, and citizenship, as well as topics such as their criminal background, health status, and whether they have overstayed a visa on a previous trip. While this information is certainly personal, the material associated with an individual's online presence can reveal a much deeper insight into a person's personality, preferences, ideas, and values. And the nature of social media technology in particular also exposes information about other people in their networks.

International travelers rely on social media and apps to find and purchase flights and accommodations, to find information about Customs procedures, to read and write travel reviews, to follow local news and make new connections, to communicate over long distances with colleagues, friends, and family back home, to contact their embassies or consular services in an emergency, and more. The DHS proposal would, in effect, ask travelers to give CBP a window into all of these online activities without clear standards for protecting those who disclose their online profiles and those in their networks.

Moreover, travelers may not be fully aware of the entire scope of information that they are disclosing. Many internet users have multiple social media accounts, sometimes dating back a decade or more. Visitors may list these outdated accounts, forgetting they contain posts and connections that are out of date. And even if a person withholds particular identifiers that are associated with sensitive content (e.g., a Grindr profile) or connections (e.g., a controversial Facebook group), investigators may be able to unearth these accounts based on the information that is disclosed.

Further, accounts on some social media sites routinely display third-party posts and comments that were added to the account owner's page without her knowledge or consent. Depending on the user's privacy settings, some of these posts could be from complete strangers. Such posts may contain inaccurate or deliberately misleading information. Social media login credentials can also be compromised, and accounts hijacked, to disseminate content that the person did not or would not post.[9]

A person's social media activity also necessarily reveals information about people in her social networks, including her family members, friends, and "followers"; therefore, disclosing a social media identifier to DHS could subject a person's close and distant associates to invasive scrutiny and exposure without their consent. This could create particular risks for journalists, lawyers, clergy, human rights workers, and others whose professions require confidentiality or who may face serious consequences if their social media profile were taken out of context. The recent experiences of a Wall Street Journal reporter pressured to give CBP access to her mobile devices[10] and an Al Jazeera journalist discovering

[9] See, e.g., Kate Conger, How activist DeRay Mckesson's Twitter account was hacked, Tech Crunch (June 10, 2016), https://techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-account-was-hacked/.
[10] Joseph Cox, WSJ Reporter: Homeland Security Tried to Take My Phones at the Border, Vice Motherboard (July 21, 2016), http://motherboard.vice.com/en_uk/read/wsj-reporter-homeland-security-tried-to-take-my-phones-at-the-border.

he was placed on an NSA watch list[11] highlight the risks such surveillance programs pose to civil society institutions including the free press.

Social media posts are also vulnerable to interpretive error. The content and conversation on a person's page or feed is highly context-dependent, making it prone to misinterpretation—particularly when the interpreter does not speak the language or lacks cultural, colloquial, or idiosyncratic touchstones necessary for accurate understanding of the content. Similarly, metadata, including contacts within a person's list of "followers" or "follows," can be easily misconstrued when divorced from the context of the connection. Without the contextual understanding that a person is a journalist or human rights researcher, for instance, her connection to violent extremist accounts could appear suspect.[12] People collect many diverse social media connections, and may not even be aware of the identity behind an account that they follow. In fact, one study found that the *majority* of friendships on Facebook are not based on a "real", non-casual relationship.[13] These features undermine the value of this data and increase the risk of erroneous denial of a visitor's ESTA application.

Finally, the proposal does not protect applicants from the risk of improper conclusions based on declining to disclose "online presence" indicators. If DHS discovers the existence of an undeclared account, will the applicant be flagged for additional scrutiny? Will CBP officials draw negative inferences from the privacy settings an applicant has placed on his accounts? These questions remain unanswered. The proposal describes no recourse for individuals who believe they were improperly denied a visa waiver, or subsequent visa application, based on their online presence.

III. Collecting online identifiers from visitors to the U.S. would be a significant expansion of U.S. intelligence activity.

This proposal seeks to implement an intelligence-gathering program in the form of a Customs administration mechanism, under the auspices of the Paperwork Reduction Act. Data collected through the I-94W and ESTA forms is not limited to determining an applicant's eligibility for a visa waiver. DHS engages in massive collection and analysis of open-source data[14] and has invested in

---

[11] Cora Currier, Glenn Greenwald, & Andrew Fishman, U.S. Government Designated Prominent Al Jazeera Journalist as "Member of al Qaeda," Intercept (May 8, 2015), https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/.

[12] Human Rights Watch, With Liberty to Monitor All: How Large-Scale U.S. Surveillance is Harming Journalism, Law and American Democracy, July 2014, *available at* https://www.aclu.org/report/liberty-monitor-all-how-large-scale-us-surveillance-harming-journalism-law-and-american.

[13] R.I. Dunbar, Do online social media cut through the constraints that limit that limit the size of offline social networks?, Royal Society: Open Science, January 2016, *available at* http://rsos.royalsocietypublishing.org/content/3/1/150292.

[14] *See* Office of Inspector General, Dep't of Homeland Security, DHS Uses Social Media To Enhance Information Sharing and Mission Operations, But Additional Oversight and Guidance Are Needed, No. OIG-13-115 (September 2013), *available at* https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-115_Sep13.pdf.

systems of automated social media analysis.[15] Increased collection and retention increases the risk of data breach, as well as the potential for misuse and abuse. Harassment and fraud are among the biggest risks to users and institutions, such as banks or hospitals, when social media identifiers are breached.[16]

Further, all of the information collected through the visa-waiver program is shared, in bulk, with U.S. intelligence agencies and will be used to seed more intelligence surveillance unrelated to the applicant's eligibility for a visa waiver.[17] If this proposal is adopted, social media identifiers – tied to the true identity of visa-waiver applicants – will be shared with the National Security Agency which can then use the information to target applicants for surveillance. Data collected under this proposal would feed into intelligence surveillance for much broader purposes and without meaningful controls. Once in the Intelligence Community (IC), elements of the IC can then use the information provided to pursue their missions. This data is likely to be used to augment existing lists and databases for tracking persons of interest to law enforcement and intelligence agencies, with consequences for innocent individuals swept up in those surveillance programs. And to the extent the applicant's social media account reveals those with whom the applicant communicates (see discussion above), those persons can be targeted as well.

Under current law, Visa Waiver Program travelers – by definition, non-U.S. persons outside the United States – who are affected by expanded surveillance under this proposal will have no recourse against abuse. Specifically, surveillance under Executive Order 12333 is conducted without any judicial oversight. It can be conducted to collect "foreign intelligence information," which includes information about the "activities" of any non-American abroad. Collection of information about these broadly defined "activities" is permissible even if there is no reason to believe that those activities threaten U.S. national security, are relevant to U.S. foreign policy, or are conducted by a person who is an agent of foreign power. Likewise, surveillance under Section 702 of the Foreign Intelligence Surveillance Act proceeds without meaningful judicial authorization, for broadly defined purposes, and regardless of whether there is information indicating that the target of surveillance is a criminal, a threat, or an agent of a foreign power. As non-U.S. persons, prospective travelers have only limited Privacy Act

[15] Ellen Nakashima, DHS monitoring of social media worries civil liberties advocate, Wash. Post (Jan. 13. 2013), https://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gIQANPO7wP_story.html.

[16] Tracy Kitten, Social Media Plays Key Role in Bank Fraud, Data Breach Today (Aug. 3, 2016), http://www.databreachtoday.com/interviews/social-media-plays-key-role-in-bank-fraud-i-3277.

[17] *See, e.g.,* Department of Homeland Security, Privacy Impact Assessment Update Electronic System for Travel Authorization (ESTA), DHS/CBP/PIA-007(f), June 20, 2016, at 5, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-june2016_0.pdf ("CBP will continue to share ESTA information in bulk with other federal Intelligence Community partners (e.g., the National Counterterrorism Center), and CBP may share ESTA on a case-by-case basis to appropriate state, local, tribal, territorial, or international government agencies.").

protections under the Judicial Redress Act, and these do not provide a guarantee against intelligence surveillance that targets an individual's expressive activity.

The community impacts of this proposal will go far beyond the denial of an individual traveler's visa-waiver application. Data collection and data sharing within the government imposes serious privacy costs that fall disproportionately on certain groups.[18] Social networks, in particular, lend themselves to association fallacies that can impact entire communities. Persons who are, or are presumed to be, of Muslim faith or Arab descent already face a disproportionate risk of religious and ethnic profiling while traveling, including enhanced TSA screening measures, wrongful inclusion on national security watchlists, and discriminatory citizen complaints.[19] Including travelers' usernames, posts, and social media affiliations in the screening process will increase the dangers of "flying while Muslim," particularly where cultural and linguistic barriers create an elevated risk of misunderstanding. A traveler who is wrongfully denied a visa waiver because of a distinct Arabic name or theological posts will suffer unfair and unjustified travel delays. And, in the process, her social media friends and followers will also be swept up in social media profiling. To the extent that the traveler's social network overlaps with her religious and ethnic community, those individuals will also be exposed to increased scrutiny and its consequences for safety and privacy.

IV. Americans will be swept up in social media collection and surveillance activities at home, and will face reciprocal disclosures requirements abroad.

If this proposal is adopted, it will disproportionately affect Arab-Americans and Muslim Americans whose family members, guests, colleagues, and business associates are flagged or denied a visa waiver as a result of their online presence. Moreover, DHS – and, by extension, the rest of the Intelligence Community – will necessarily acquire information about Americans whose accounts are affiliated with those scrutinized and flagged profiles.

This proposal would create significant risks of ideological profiling, if travelers are subjected to elevated scrutiny merely because they have expressed a strongly-held religious or political belief

[18] See, e.g., Alvaro M. Bedoya, The Color of Surveillance, Slate (Jan, 18, 2016), http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html.

[19] American travelers have been plagued by profiling based on skin color, language, attire, and other markers of religious and ethnic background. See, e.g., Catherine Rampell, Ivy League economist ethnically profiled, interrogated for doing math on American Airlines flight, Wash. Post (May 7, 2016), https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doing-math-on-american-airlines-flight/?tid=a_inl&utm_term=.00e58cfbfc37; Peter Holley, Muslim couple says they were kicked off Delta flight for using phone, saying 'Allah,' Wash. Post (Aug. 7, 2016), https://www.washingtonpost.com/news/morning-mix/wp/2016/08/07/muslim-couple-says-they-were-kicked-off-delta-flight-for-using-phone-saying-allah/?tid=a_inl; Carma Hassan & Catherine E. Shoichet, Arabic-speaking student kicked off Southwest flight, CNN.com (Apr. 8, 2016), http://www.cnn.com/2016/04/17/us/southwest-muslim-passenger-removed/.

online. Ideological exclusion of visitors would deny Americans access to information and opportunities for cultural and educational exchange that spur creativity and innovation. And American businesses would suffer economic impacts when foreign scholars, colleagues, and investors are delayed or denied entry. Potential visitors may decide instead to censor themselves online, rather than risk exclusion, which would further diminish Americans' access to information and opportunity for informed debate. As a network, the value of the global internet is related to the size and engagement of its participants; withdrawal of certain groups or communities diminishes the value of a network for all members.[20]

Finally, if this proposal is enacted, Americans will likely face reciprocal social media disclosure requirements when traveling abroad. Customs and immigration policy is notoriously susceptible to reciprocity effects, and the U.S. Visa Waiver Program is no exception. Currently, for example, the European Commission is considering restricting visa-free travel for Americans and Canadians in response to the absence of a visa-waiver path for nationals of some EU member states.[21] Americans traveling to Iran, Iraq, Syria, or Sudan could face higher hurdles, including social media disclosure requirements, in retaliation for the U.S. decision to exclude any recent travelers or dual nationals of those countries from eligibility for a visa waiver.[22] And all countries could be incentivized to implement online identity disclosures in the event that the U.S. expands its social media inquiry to visa applications.

For Americans traveling abroad, reciprocal social media disclosure requests could create travel delays and legal risk for speech that is protected under the United States Constitution. In non-visa waiver countries with fewer legal safeguards, disclosure requirements could expose American travelers to serious consequences such as border interrogations, administrative detentions, and other more serious penalties for social media activity that offends customs or norms against homosexuality, female immodesty, or religious or ideological dissent.[23] Other states' use of social media screening as an element of border security has demonstrated the significant risk of ideological and ethnic profiling that these programs create.[24] For example, in 2014, the U.S. Consulate in Jerusalem noted that "U.S. citizen visitors have been subjected to prolonged questioning and thorough searches by Israeli

---

[20] *See* Yochai Benckler, Wealth of Networks: How Social Production Transforms Markets and Freedom (2007).
[21] Tara Palmeri & Maïa de la Baume, EU considers restricting visa-free travel for Americans, Canadians, Politico (Apr. 7, 2016), http://www.politico.eu/article/eu-considers-restricting-visa-free-travel-for-americans-canadians/. The U.S. sets visa policy on a country-by-country basis; some EU members are not part of the U.S. Visa Waiver Program. This has led the European Commission to re-examine its visa policies for the United States. *Id.*
[22] Paul Dallison, U.S. visa changes hit Europeans, Politico (Jan. 22, 2016), http://www.politico.eu/article/us-visa-changes-hit-europeans-dual-nationality-iran-iraq-syria/.
[23] *See, e.g.,* the case of British national Stephen Comiskey, who was reportedly entrapped by Saudi police, jailed, and sentenced to death for homosexuality before the United Kingdom managed to negotiate his release. Nick Parker, Execution fear of gay Brit battered in Saudi, theSun.co.uk (Mar. 31, 2011), https://www.thesun.co.uk/archives/news/463707/execution-fear-of-gay-brit-battered-in-saudi/. Singapore, which also criminalizes same-sex sexual relations, is a visa-waiver country.
[24] Diaa Hadid & Joseph Federman, Israel asks Arab visitors to open emails to search, NBCNews.com (June 5, 2012), http://www.nbcnews.com/id/47690140/ns/world_news-mideast_n_africa/t/israel-asks-arab-visitors-open-emails-search/.

authorities upon entry or departure. Those whom Israeli authorities suspect of being of Arab, Middle Eastern, or Muslim origin [...] may face additional, often time-consuming, and probing questioning by immigration and border authorities, or may even be denied entry into Israel or the West Bank."[25] All Americans have an interest in ensuring that social media border-screening programs do not become an international norm.

V. Online identifier collection would be ineffective and will impose significant unaccounted costs.

DHS indicates that collection of visa-waiver applicants' online identity information will "enhance the existing investigative process" for screening visa-waiver applicants.[26] DHS has previously argued that generally increasing ESTA data-collection will streamline the visa-waiver application process by reducing the number of false-positive matches between applications and terrorism watchlists.[27] These empirical arguments rest on several flawed assumptions.

First, the ease of circumvention undermines this program's utility. Individuals who pose a threat to the United States are highly unlikely to volunteer online identifiers tied to information that would raise any question about their admissibility to the United States. Such questioning is far more likely to yield a flood of profiles from unsuspecting travelers who feel compelled to disclose information. It may also prompt some travelers to create false or "dummy" accounts to shield their privacy—or to deliberately undermine CBP agents' investigations.

Second, sorting through the quantity of information included in an individual's online presence creates a tremendous and costly administrative burden. Information traditionally collected as part of the visa process (names, birthdates, and place of birth, for example) includes single data points that can be easily cross-referenced against prepared indices such as watchlists or hotspots for terrorism or infectious diseases. By contrast, social media identifiers will yield messy and multidimensional data sets. As discussed above, social media in particular is vulnerable to misinformation and misinterpretation errors. Further, one identifier can expand the available data by many orders of magnitude with no comparable qualitative increase in information or intelligence. Given that the average internet user has five social media profiles,[28] this proposal would introduce significant noise and little if any discernable signal to the visa-waiver screening process.

---

[25] U.S. Consulate in Jerusalem, Entering and Exiting Jerusalem, the West Bank, and Gaza, https://jru.usconsulate.gov/u-s-citizen-services/local-resources-of-u-s-citizens/entering-exiting/; *see also* Adam Taylor, These accounts from Arab Americans show why an Israeli visa waiver plan is so controversial, Wash. Post (Apr. 27, 2014), https://www.washingtonpost.com/news/worldviews/wp/2014/04/27/these-accounts-from-arab-americans-show-why-an-israeli-visa-waiver-plan-is-so-controversial/ .

[26] Federal Register Notice, *supra* n.1.

[27] U.S. Customs & Border Protection, Strengthening Security of the VWP through Enhancements to ESTA, https://www.cbp.gov/travel/international-visitors/esta/enhancements-to-esta-faqs.

[28] Jason Mander, Internet users have average of 5.54 social media accounts, GlobalWebIndex.net (Jan 23, 2015), http://www.globalwebindex.net/blog/internet-users-have-average-of-5-social-media-accounts. Moreover, the

Third, transforming raw social media data into actionable intelligence will require new capabilities in machine learning and complex network analytics—increasing costs and introducing new sources of error into the screening process. There may be useful data points that could produce insights or investigative leads amid the deluge of irrelevant and potentially false information gathered in response to this question. But, given the complexity of the dataset, CBP officers cannot conduct a cursory analysis. Even in combination with simple algorithmic screening against prepared databases and indices, this type of analysis is minimally accurate. Currently, machine learning used to identify jihadist accounts on Twitter exhibits an error rate of 10 to 24 percent.[29] Such an error rate would represent between 2 and 5 million annual visitors being falsely flagged under the Visa Waiver Program.[30] And because these algorithms are biased against foreign languages, particularly those not based on the Roman alphabet, the error rate for algorithmic assessment of social media information collected under this proposal will likely be even higher. By using unreliable and misleading social media activity as a proxy for admissibility, DHS will experience an increase in incidence of false-positive error.[31]

Moreover, machine learning can also introduce false negatives into a risk assessment. For example, if an algorithm is trained to identify whether an applicant is a person of interest, a positive match between an applicant's name and biographical information and an identity on a terrorism watchlist will result in a red flag. However, when social media information is added to the evaluation, there is a risk that it can contradict or discredit a database match, removing a correctly identified red flag from the application.[32] Given that machine learning processes introduce serious risks of both false-positive and false-negative signals, the necessity of human review cannot be avoided.

The more deeply a CBP investigator delves into an applicant's social media profile, however, the more training and context she will need in order to overcome the interpretive errors inherent in social media content and connection analysis. Some of the best technology in use today for identifying ISIS accounts

---

average social media user posts frequently and has the ability to post various types of data. A majority of Facebook, Instagram, and Twitter users post at least once per week. Maeve Duggan et. al, Frequency of Social Media Use, Pew Research Center (Jan 9, 2015), http://www.pewinternet.org/2015/01/09/frequency-of-social-media-use-2/.

[29] Enghin Omer, Thesis: Using machine learning to identify jihadist messages on Twitter, Uppsala University, Sweden, July 2015, http://uu.diva-portal.org/smash/get/diva2:846343/FULLTEXT01.pdf.

[30] 2014 Yearbook of Immigration Statistics, *available at* https://www.dhs.gov/sites/default/files/publications/table28d_7.xls.

[31] Sarah Foxen & Sarah Bunn, Forensic Language Analysis, 509 POSTnote (Sept. 2015), http://www.forensiclinguistics.net/POST-PN-0509.pdf.

[32] This effect is a byproduct of algorithmic decisionmaking: Risk-assessment algorithms rely on various qualifying criteria to determine whether an entry can be identified as "suspicious." If the various fields of data pertaining to an entry reinforce each other, this can increase the algorithm's accuracy. But if these fields do not reinforce each other and the standards for evaluating the contradictory information (for example, innocuous social media posts) are not clearly delineated in the algorithmic rule, then it can reduce the accuracy of the algorithm by introducing false-negative error in the "suspicion" assessment.

includes automated analysis and human review and has a margin of error at 2.54 percent.[33] While this may first appear to be trivial, in practical effect it would mean nearly half a million visitors to the U.S. were denied a visa waiver, subject to significant additional scrutiny, and potentially deterred from visiting the U.S. every year. The combined effect of more error and more human review will result in substantial additional labor costs, which are not reflected in the DHS's estimated cost to the public of $265 million for the ESTA program proposal.[34]

* * *

DHS's proposal to collect the online identifiers of travelers under the Visa Waiver Program is highly invasive and will chill free expression online, will disproportionately affect Muslim and Arab communities within and outside the U.S., will lead to reciprocal burdens for Americans travelling abroad, and will be ineffective and prohibitively expensive. We urge DHS to withdraw the proposal.

Respectfully submitted,

Nuala O'Connor
Emma Llansó
Rita Cant
Greg Nojeim
Michelle de Mooy
Aislinn Klos
Apratim Vidyarthi

Center for Democracy & Technology

[33] J.M. Berger & Jonathon Morgan, The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter 46, Brookings Inst., March 2015, http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

[34] See Federal Register Notice, *supra* n.1. Under the Paperwork Reduction Act, annual cost burden estimates do not include labor cost for the estimated burden-hours for a proposal. U.S. Office of Personnel and Management, Paperwork Reduction Act Guide 2.0, 39, OPM.gov (April 2011), *available at* https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf.