



Internet Association

The Internet Association (IA) submits these comments in connection with the Department of Homeland Security's (DHS) proposal to request that individuals entering the U.S. on visa waivers supply social media identifiers. The IA represents 40 of the world's leading internet companies.¹

While the IA understands both the national security policy behind the DHS proposal as well as the voluntary nature of the information requested, our members have concerns about the precedent setting nature of the proposal as currently drafted. These concerns include:

- The spillover effects of the proposal on human rights and civil liberties globally;
- The scope of the data requested; and
- The uses to which the data will be put.

Human Rights and Civil Liberties Implications

As global companies with billions of end-users around the world, the Internet Association members' primary concern with the proposal is its precedent setting nature for social media identifiers.

Should the U.S. Government advance with the DHS proposal it is probable that other countries will make similar requests of visitors entering their country, including U.S. citizens. This will be true for democratic and non-democratic countries alike, including those that do not have the same human rights and due process standards as the U.S. Additionally, these other countries are likely to cite to the U.S.'s voluntary scheme but make information requests mandatory.

Before moving forward with this policy, the U.S. Government should consider its likely impact on both those visiting the U.S. and others traveling around the world, to countries that implement similar policies. As currently drafted, it is possible that the proposal will have a chilling effect on use of social media networks, online sharing and, ultimately, free speech online.

The Scope of Data Requested

The information sought by DHS about visitors' "online presence" is not clearly defined in the notice as currently drafted, and includes "social media identifiers" associated with a wide range of Internet-based "provider[s] /platform[s]."

As more of an individual's personal life takes place online, the number of every day services for which there is a digital service provider is significant. Consequently, the amount of information any one individual could supply to DHS is considerable. Although the DHS already requests a range of personal data on entry into the U.S., a person's online identifiers are qualitatively different from other data requested. Online identifiers provide access to a person's opinions, beliefs, identity and community. Further, identifiers can - at times - highlight

¹ The Internet Association's members include Airbnb, Amazon, Coinbase, DoorDash, Dropbox, eBay, Etsy, Expedia, Facebook, FanDuel, Google, Groupon, Handy, IAC, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Pinterest, Practice Fusion, Rackspace, reddit, Salesforce.com, Snapchat, Spotify, SurveyMonkey, Ten-X, TransferWise, TripAdvisor, Turo, Twitter, Uber Technologies, Inc., Yahoo!, Yelp, Zenefits, and Zynga.



information on gender and sexuality. While requesting social media identifiers - which may be available publicly - may not in itself be considered a significant increase in requested data, the additional insight provided into a visitor's life by providing these identifiers is significant.

The Use and Development of Data Collected

According to the DHS consultation, '[c]ollecting social media data will enhance the existing investigative process and provide DHS greater clarity and visibility to possible nefarious activity and connections by providing an additional tool set which analysts and investigators may use to better analyze and investigate the case.'

While the Internet Association supports the national security objective underpinning the DHS proposal, it is unclear from the notice how DHS would seek to achieve this goal. Analysis of all applicants' social media "activity and connections" would be costly and difficult. This cost does not appear to be factored into DHS' analysis. Asking social media platforms, including IA members, to provide additional information would be an unnecessary and disproportionate burden.

We are also concerned that a declaration on a visa waiver form of ownership of a username will be taken as fact by the DHS. Companies should not be compelled to treat a naked, offline claim of account ownership on a visa waiver form as sufficient or conclusive proof that a particular individual owns an account. Our experience has shown us that offline representations of account ownership are ripe with typographical errors and/or fraud.

If DHS or other agencies treat representations of account ownership as fact, companies may be compelled to disclose user data that - in some instances - pertains to a user other than the visa waiver applicant. DHS should be cognizant of and address this serious privacy concern by clarifying that claims of ownership over a social media identifier will not be treated as conclusive and/or override authentication mechanisms companies have established when responding to legal process.

We look forward to DHS's response to the consultation process and welcome the opportunity to take part in this process.