Jonathan Cantor
Acting Chief Privacy Officer
Privacy Office
Department of Homeland Security
Washington, DC 20528-0655
Via Federal e-Rulemaking Portal: http://www.regulations.gov

October 3, 2016

Re: Docket Number DHS-2016-0054

To whom it may concern:

The undersigned groups write to convey their concerns regarding the updated notice for the System of Records titled "DHS/U.S. Customs and Border Protection (CBP)-009 Electronic System for Travel Authorization (ESTA) System of Records."[1] Some of these same groups submitted comments to U.S. Customs and Border Protection pursuant to the Paperwork Reduction Act regarding the Department of Homeland Security's proposed policy to collect social media information from travelers seeking entry to the United States through the Visa Waiver Program (VWP), which we incorporate here by reference.[2] In light of the revised System of Records Notice (SORN) for ESTA, posted on September 2, 2016, as well as related explanatory documents, we submit these comments to highlight our continued objections to the DHS's proposal to request social media identifiers from VWP travelers.

Overbroad collection of Americans' data: The SORN states that social media information is being gathered to address "ongoing national security concerns surrounding foreign fighters exploiting the VWP."[3] While the social media collection is ostensibly directed at non-U.S. citizens traveling from

[1] Privacy Act of 1974; Department of Homeland Security, U.S. Customs and Border Protection--009 Electronic System for Travel Authorization System of Records, 81 Fed. Reg. 60,713, *available at* https://www.regulations.gov/document?D=DHS-2016-0054-0001.

[2] *See*, *e.g.*, Letter from Faiza Patel, Co-Director, and Rachel Levinson-Waldman, Senior Counsel, Liberty and National Program, Brennan Center for Justice, to U.S. Customs and Border Protection (Aug. 22, 2016), *available at* https://www.regulations.gov/document?D=USCBP-2007-0102-0588; Letter from Emma Llanso, Center for Democracy & Technology, on behalf of Twenty-Eight Human Rights and Civil Liberties Organizations, to U.S. Customs and Border Protection (Aug. 22, 2016), *available at* https://www.regulations.gov/document?D=USCBP-2007-0102-0590 [hereinafter "Letter from Twenty-Eight Civil Liberties Organizations"]; Letter from Emma Llanso, Center for Democracy & Technology, to U.S. Customs and Border Protection (Aug. 22, 2016), *available at* https://www.regulations.gov/document?D=USCBP-2007-0102-0625; Letter from Sophia Cope, Staff Attorney, Electronic Frontier Foundation, to U.S. Customs and Border Protection (Aug. 22, 2016), *available at* https://www.regulations.gov/document?D=USCBP-2007-0102-0586; *see also* Sophia Cope, *CBP Fails To Meaningfully Address Risks of Gathering Social Media Handles*, ELECTRONIC FRONTIER FOUNDATION (Sept. 14, 2016), https://www.eff.org/deeplinks/2016/09/cbp-fails-meaningfully-address-risks-gathering-social-media-handles.

[3] Fed. Reg., *supra* note 1, at 60,714.

VWP countries, however, DHS/CBP will collect information about U.S. citizens in a variety of ways.

First, the Privacy Impact Assessment (PIA) accompanying the SORN indicates that the agency may take into account "information posted by an associate of the applicant on the applicant's social media page."[4] Millions of tourists and businesspeople travel to the United States from VWP program countries every year; many of these travelers are likely to have business associates, family, and friends in the U.S., and many of them will communicate with their contacts in the U.S. over social media. This data collection could therefore vacuum up a significant amount of data about Americans' associations, beliefs, religious and political leanings, and more, chilling First Amendment freedoms.[5] Indeed, the PIA acknowledges that DHS/CBP is likely to collect First Amendment-protected information as part of this program.[6]

Second, in addition to permitting agents to monitor postings, the PIA indicates that CBP will conduct link analysis on applicants, enabling the agency to "identify direct contacts (such as an ESTA applicants [sic] "friends," "followers," or "likes"), as well as secondary and tertiary contacts associated with the applicant that pose a potential risk to the homeland or demonstrate a nefarious affiliation on the part of the applicant."[7] In plain English, it appears that even if a friend or associate has not directly interacted with the applicant on social media, the agency will ferret out connections; if a "follower" of an applicant raises a red flag for the agency, the applicant herself may be denied permission to travel to the United States.

This process will allow DHS/CBP to collect even more information about Americans, since it will sweep in not only those who voluntarily interact in some way with VWP applicants on social media but also those who are simply connected to them, even if only tangentially. It also invests CBP agents with unchecked discretion to determine what constitutes a "risk to the homeland" or a "nefarious affiliation," terms that are undefined in the public materials; opens up opportunities for malefactors or mischief-makers to compromise a traveler's application simply by following the applicant on social media; and threatens to overwhelm the agency with information about applicants' third-degree contacts, most of which are likely to have little relevance to their fitness to travel to the United States.

Overbroad retention and sharing: Second, the SORN authorizes the retention and sharing of significant amounts of Americans' data for purposes far beyond the initial reason for collection.

Where DHS/CBP determines that communications with Americans are "relevant to making an ESTA determination," the agency will retain those records.[8] Both derogatory and innocuous information could be deemed relevant to the ESTA determination, resulting in a substantial quantity

---

[4] DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT UPDATE FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION 4 (2016), [hereinafter PRIVACY IMPACT ASSESSMENT], *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-september2016.pdf.
[5] See Kaveh Waddel, *How Surveillance Stifles Dissent on the Internet*, THE ATLANTIC (Apr. 5, 2016), http://www.theatlantic.com/technology/archive/2016/04/how-surveillance-mutes-dissent-on-the-internet/476955/.
[6] PRIVACY IMPACT ASSESSMENT, *supra* note 4, at 3.
[7] *Id.* at 5.
[8] *Id.* at 4.

of innocent Americans' data being retained within ESTA. Moreover, the SORN authorizes DHS/CBP to share data with a range of partners – local, state, tribal, federal, and foreign – for a variety of purposes, both in bulk and on a case-by-case basis.[9] This sharing authority is quite broad; the information can be disclosed, as a routine use, in the following circumstances:

> To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.[10]

According to the SORN, this routine use was expanded in order to clarify that "DHS may share information when it determines that the information would *assist* in the enforcement of civil or criminal matters, and not only when the record itself facially indicates a violation or potential violation of law."[11]

This is an extremely broad mandate for sharing that appears to have only the most tangential connection to the national security justification articulated in the SORN. Instead, it will enable DHS/CBP to share data with the FBI and other agencies for a multitude of purposes with no relationship to legitimate national security concerns. It also increases the risk that law enforcement agencies from other countries could request and use social media information to stifle democracy or dissent, simply by citing a "criminal, civil or regulatory violation" to which the data is colorably related – not a far-fetched concern.[12]

Moreover, while data produced via link analysis evidently will not be stored in ESTA, it will be stored in the Automated Targeting System (ATS),[13] a vast database of travel information that is almost entirely exempted from the Privacy Act, including the requirement that the data be "relevant and necessary."[14]

Lack of transparency: Finally, the PIA indicates that CBP staff at the National Targeting Center (NTC) will be authorized to open social media accounts and use screen names that do not reflect their DHS affiliations, contrary to usual agency rules.[15] While agents are prohibited from interacting with other social media users, including by "friending," "fan-ing," "liking," or "messaging" them, it is unclear whether they could "follow" users on platforms like Twitter and Instagram using misleading account or screen names. This practice also raises questions regarding the ability of the

---

[9] Fed. Reg., *supra* note 1, at 60,714; Letter from Twenty-Eight Civil Liberties Organizations, *supra* note 2; Llanso, *supra* note 2.
[10] Fed. Reg., *supra* note 1, at 60,717.
[11] *Id.* (emphasis added).
[12] *See*, *e.g.*, *Turkish Leader Using Slander Law to Stifle Dissent, Say Critics*, DUNYANEWS TV (March 5, 2015), http://dunyanews.tv/en/World/265323-Turkish-leader-using-slander-law-to-stifle-dissent; Alissa de Carbonel, *Putin Is Building a 'Virtual Iran Curtain' To Stifle Online Dissent,* BUSINESS INSIDER (Sept. 4, 2014 5:51 AM), http://www.businessinsider.com/r-putin-plays-cat-and-mouse-with-russian-online-critics-2014-9.
[13] PRIVACY IMPACT ASSESSMENT, *supra* note 4, at 5.
[14] Privacy Act of 1974, 5 U.S.C. § 552a (e) (1).
[15] PRIVACY IMPACT ASSESSMENT, *supra* note 4, at 5.

public to monitor this program adequately; if it is impossible to identify new followers as DHS/CBP employees, it will also be impossible to determine whether the agency engages in profiling in determining whom to follow, or violates its internal rules by liking or messaging its targets. In light of the significant discretion accorded to CBP officers in determining whom to investigate, this is a recipe for abuse; at the very least, both the rules for utilizing social media and the mechanisms for oversight and accountability should be clarified.

In sum, we believe the new materials released by the Department, including the Systems of Records Notice and the Privacy Impact Assessment, do little to mitigate or resolve the significant problems already raised by civil society organizations. We therefore urge the Department of Homeland Security to withdraw its plan to permit the collection of information from, and expansion of routine uses for, social media. For any questions about this submission, please contact Rachel Levinson-Waldman, Senior Counsel to the Liberty and National Security Program at the Brennan Center for Justice, at rachel.levinson.waldman@nyu.edu or 202-249-7193.

Sincerely,

American Civil Liberties Union
Advocacy for Principled Action in Government
Bill of Rights Defense Committee & Defending Dissent Foundation
Brennan Center for Justice
Center for Democracy and Technology
Center for Media Justice
Council on American-Islamic Relations
Electronic Frontier Foundation
New America's Open Technology Institute
OpenTheGovernment
Restore the Fourth