epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY
U.S. CUSTOMS AND BORDER PROTECTION

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

30-Day Notice and Request for Comments; Revision of an Existing Collection of Information

[1651-0111]

September 30, 2016

By a Notice and Request for Comments published on June 23, 2016, the Department of Homeland Security ("DHS"), Customs and Border Protection ("CBP") proposes to add the following question to the I-94W (Nonimmigrant Visa Waiver Arrival/Departure Record) form and to the Electronic System for Travel Authorization ("ESTA"):

> **Please enter information associated with your online presence—Provider/Platform—Social media identifier**.[1]

On August 31, 2016, DHS republished the Notice and Request for Comments to allow for an additional 30 days to comment.[2] Accordingly, EPIC submits these updated comments.

---

[1] Notice and Request for Comments, 81 Fed. Reg. 40892 (proposed June 23, 2016), *available at* https://www.gpo.gov/fdsys/pkg/FR-2016-06-23/pdf/2016-14848.pdf.

The agency states, "collecting 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." DHS has provided little other details about the use of the social media identifiers it plans to collect.

Pursuant to DHS's Notice and Request for Comments, the Electronic Privacy Information Center ("EPIC") submit these comments to urge the agency to: (1) withdraw its proposal to collect social media identifiers; and (2) review the appropriateness of the agency's current use of social media analysis.

I. Introduction

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment, and constitutional values.[3] EPIC has a particular interest in preserving the right of people to engage in First Amendment protected activities without the threat of government surveillance.

EPIC previously sued DHS to obtain documents related to a DHS social network and media monitoring program.[4] These documents revealed that the agency had paid over $11 million to an outside company, General Dynamics, to engage in monitoring of social

---

[2] Notice and Request for Comments, 81 Fed. Reg. 60014 (proposed August 31, 2016), *available at* https://www.gpo.gov/fdsys/pkg/FR-2016-08-31/pdf/2016-20929.pdf.
[3] EPIC, *About EPIC* (2016), https://epic.org/epic/about.html.
[4] EPIC, *EPIC v. Department of Homeland Security: Media Monitoring*, https://epic.org/foia/epic-v-dhs-media-monitoring/.

networks and media organizations and prepare summary reports for DHS.[5] According to DHS documents, General Dynamics would "monitor public social communications on the Internet," including the public comments sections of NYT, LA Times, Huff Po, Drudge, Wired's tech blogs, and ABC News.[6] DHS also requested monitoring of Wikipedia pages for changes[7] and announced its plans to set up social network profiles to monitor social network users.[8]

DHS required General Dynamics to monitor not just "potential threats and hazards" and "events with operational value," but also paid the company to "identify[] reports that reflect adversely on the U.S. Government [or] DHS . . . ."[9]

Within the documents, DHS clearly stated its intention to "capture public reaction to major government proposals."[10] DHS instructed the media monitoring company to generate summaries of media "reports on DHS, Components, and other Federal Agencies: positive and negative reports on FEMA, CIA, CBP, ICE, etc. as well as organizations outside the DHS."[11]

The documents obtained by EPIC through its Freedom of Information Act lawsuit led to a Congressional hearing on DHS social network and media monitoring program.[12]

---

[5] DHS Social Media Monitoring Documents, *available at* https://epic.org/foia/epic-v-dhs-media-monitoring/EPIC-FOIA-DHS-Media-Monitoring-12-2012.pdf; *See also* Charlie Savage, *Federal Contractor Monitored Social Network Sites*, NYT (Jan. 13, 2012).
[6] DHS Social Media Monitoring Documents at 127, 135, 148, 193.
[7] *Id.* at 124, 191.
[8] *Id.* at 128.
[9] *Id.* at 51, 195.
[10] *Id.* at 116.
[11] *Id.* at 183, 198.
[12] *See DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the H. Comm. on Homeland Security*, 112th Cong. (2012).

EPIC submitted a statement for the record for that hearing opposing the agency's media monitoring and called for the immediate cease of the program.[13]

DHS now proposes collecting social media identifiers of foreigners seeking to visit the United States in order to scrutinize their social media accounts during the vetting process. EPIC opposes this proposal.

II. The Lack of Transparency Surrounding DHS's Proposal Increases the Prospect of Abuse, Mission Creep, and Disproportionate Risks for Marginalized Groups

DHS has stated that the agency will use the social media identifiers as part of the existing investigative process to screen "alien visitors for potential risks to national security and the determination of admissibility to the United States."[14] Little additional information is provided.

It is not clear how DHS intends to use the social media identifiers. In the past, DHS has monitored social and other media for dissent and criticism of the agency.[15] Will the agency monitor for similar speech that is critical of U.S. policy? Will mere dissent constitute grounds for denying entry into the U.S.? Additionally, will alien visitors who provide their social media identifiers open up their social network associations to scrutiny? How long will social media identifiers be retained and who will they be shared

[13] Marc Rotenberg, President and Ginger McCall, EPIC Open Government Project Director, *Statement for the Record for Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy* (Feb. 16, 2012), https://epic.org/privacy/socialmedia/EPIC-Stmnt-DHS-Monitoring-FINAL.pdf.
[14] 81 Fed. Reg. at 40892-893.
[15] Marc Rotenberg, President and Ginger McCall, EPIC Open Government Project Director, *Statement for the Record for Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy*, 1-3 (Feb. 16, 2012).

with? How will DHS prevent Muslim and Arab Americans from being scrutinized more harshly?

Additionally, what information will the social media identifiers be combined with? Will DHS use the social media identifiers to obtain additional information about he applicant from the social media companies? Will applicants be informed if the information obtained from their social media accounts led to the denial of their application? Answers to these questions and more need to be provided prior to any consideration of DHS inquiry into social media identifiers of people suspected of no crime.

This lack of transparency around a proposal that will scrutinize the social media accounts of individuals not suspected of any wrongdoing leaves the door open for abuse, mission creep, and the disproportionate targeting of Muslim and Arab Americans among other marginalized groups. This proposal is especially alarming in light of DHS's past monitoring of social media for dissent. DHS has provided no details of how the agency will tailor the use of social media identifiers to ensure their use does not expand beyond the stated purpose or be misused to target individuals merely engaged in First Amendment protected activities.

III. Indiscriminate Scrutiny of Social Media Accounts Chills First Amendment Protected Activities

The DHS proposal to collect social media identifiers of visiting aliens implicates the First Amendment and will have a chilling effect. Freedom of speech and expression

are core civil liberties and have been strongly protected by the Constitution and the U.S. courts.[16] These rights extend to non-U.S. citizens.[17]

The proposal states that by viewing social media accounts DHS will have more clarity and visibility into nefarious activity or connections of those applying to enter the country. However, the proposal assumes that what is on social media is really an accurate picture of a person and those that they are close with. People connect with others on social media or a number of reasons. An individual's "friend" on a social media site could range from a close friend to an acquaintance to someone they may never have met. Often individuals connect to people on social media who have completely different perspectives and world views. Furthermore, the proposal fails to state to what extent possible connections will be used in the vetting process and to what extent the social media accounts of U.S. citizens may be used as part of the vetting process.

The proposal also indicates that DHS will view users posts on social media as part of the vetting process but fails to take into account that posts on social media can be taken completely out of context. Many individuals have been on social media for years and have effectively created a permanent archive of their lives that has the potential to

[16] *See, e.g.*, *United States v. Stevens*, 130 S. Ct. 1577, 1585 (2010) (holding that the "First Amendment itself reflects a judgment by the American people that the benefits of its restrictions on the Government outweigh the costs"); *see also NAACP v. Alabama ex. rel. Patterson,* 357 U.S. 449 (1958) (finding that membership lists of political and religious organizations implicates significant First Amendment interests).

[17] *See* David Cole, *Are Foreign Nationals Entitled to the Same Constitutional Rights as Citizens?*, 25 T. Jefferson L. Rev. 367-388 (2003) ("foreign nationals are generally entitled to the equal protection of the laws, to political freedoms of speech and association, and to due process requirements of fair procedure where their lives, liberty, or property are at stake.").

come back and haunt them later.[18] Teenagers are routinely warned to be careful of what they post on social media for the implications it may have on their future,[19] however both teenagers and adults have made posts on social media which they later regret and may not be an actual reflection of who they are.[20] The same considerations should be taken into account when using social media to vet those entering the country. Social media does not necessarily reflect who a person truly is and taking posts out of context has the potential to wrongly deny people entry for an inside joke or posturing that the DHS does not understand from viewing certain information in isolation.[21] Furthermore, in addition to what is on social media the proposal runs the risk of making what is not on social media seem suspect. Some individuals may not be active on social media or may not have any social media accounts at all and the DHS has failed to say what impact, if any, this may have on the vetting process.

Government programs that threaten important First Amendment rights are immediately suspect and should only be undertaken where the government can

---

[18] danah boyd et. al., *Social Media Surveillance and Law Enforcement*, DATA & CIVIL RIGHTS, Oct. 27, 2015, http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf.

[19] Franki Rosenthal, *Caution ahead: The dangers of social media*, SUN SENTINEL, Feb. 2, 2016, http://www.sun-sentinel.com/teenlink/college/tl-caution-ahead-the-dangers-of-social-media-20160202-story.html.

[20] Alyssa Giacobbe, *6 ways social media can ruin your life*, BOSTON GLOBE, May 21, 2014, https://www.bostonglobe.com/magazine/2014/05/21/ways-social-media-can-ruin-your-life/St8vHIdqCLk7eRsvME3k5K/story.html.

[21] boyd et. al., *Social Media Surveillance*; Brandon Giggs, *Teen failed for Facebook 'joke' is released*, CNN, Jul. 13, 2013 (http://www.cnn.com/2013/07/12/tech/social-media/facebook-jailed-teen/ (discussing a teenager who was arrested after making a "threat" that, when viewed in context, appears to be sarcasm); Ellie Kaufman, *Social Media Surveillance Could have a Devastating Impact on Free Speech. Here's Why.*, MIC, Jan. 19, 2016, https://mic.com/articles/132756/social-media-surveillance-could-have-a-devastating-impact-on-free-speech-here-s-why#.7JAYtQm0V.

demonstrate a compelling interest that cannot be satisfied in other way.[22] Government programs that potentially scrutinize online comments, dissent, and criticism for the purpose of vetting alien visitors prior to entry into the U.S. send a chilling message to all users of social media—which increasingly provides important forums to share ideas, engage in debates, and explore new ideas.

Providing one's social media identifiers may be voluntary, but it is of little comfort. Most applicants will feel pressure to provide the information over concerns that withholding such information will seem suspect and reflect negatively on their application.

IV. The Demand for an Individual's Personal Identifier Raises Particular Privacy Concerns

The request for "social media identifiers" raises a related concern – this particular type of personal information is the key that ties together discrete bits of personal data.[23] In the past, the United States has sought to regulate the collection and use of the Social Security Number precisely because of the concern that is leads to government profiling.[24] More recently, the availability of the SSN has been shown to contribute to identity theft and financial fraud.[25]

---

[22] *See, e.g.*, *NAACP v. Button*, 83 S. Ct. 328 (1963); *Citizens United v. Fed. Election Comm'n*, 130 S. Ct. 876 (2010).
[23] *Social Security Numbers*, EPIC, https://epic.org/privacy/ssn/.
[24] *See Use of Social Security Number as a National Identifier, Before the Subcomm. on Social Security of the House Comm. on Ways and Means*, 102nd Cong. (1991) (statement of Marc Rotenberg, Computer Professionals for Social Responsibility; Privacy Act of 1974, 5 U.S.C. §552a (2016).
[25] FTC, Security in Numbers: SSNs and ID Theft (Dec. 2008), https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf.

A social media identifier is not private in the sense that it is a secret. But the collection of a social media identifier by the government does raise privacy concerns because it enables enhanced profiling and tracking of individuals.

For this reason, as well, we urge the agency to withdraw the proposal.

V. EPIC Recommendations

The problems with collecting social media identifiers and scrutinizing the social media accounts of persons not suspected of any wrongdoing are significant and far-reaching. DHS has provided little transparency in how the agency plans to use social media identifiers collected from alien visitors. Such opaqueness in DHS's proposal to collect social media identifiers provides little comfort that DHS will provide the transparency necessary to ensure that the program is subject to appropriate oversight and accountability.

EPIC urges DHS to withdraw its proposal to collect social media identifiers from alien visitor applicants. Additionally, EPIC recommends that any current use of social media analysis by DHS should be reviewed to determine whether it is necessary, whether it undermines First Amendment protected activities, and to determine what safeguards are in place and if the safeguards ensure appropriate oversight and public transparency.

VI. Conclusion

EPIC respectfully requests that DHS reconsider its proposal to collect social media identifiers. The proposal is contrary to First Amendment rights of speech, expression, and association.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Jeramie D. Scott
EPIC National Security Counsel

Kim Miller
EPIC Fellow