

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

CUSTOMS AND BORDER PROTECTION

Agency Information Collection Activities: Electronic Visa Update System

[Docket No. 2017-08505]

May 30, 2017

By notice published April 27, 2017 U.S. Customs and Border Protection (“CBP”) proposes to revise an existing collection of information.¹ CBP proposes to ask individuals to disclose information associated with their online presence, including social media identifiers.

The agency claims it is requesting this information to help review visa applicants and to provide a method to contact applicants.”² CBP has provided little additional information about the use of the social media identifiers the agency plans to collect.

Pursuant to the agency’s request for comments, the Electronic Privacy Information Center (“EPIC”) submit these comments to urge the Department to: (1) withdraw its proposal to collect social media identifiers; and (2) review the appropriateness of using social media to make visa determinations.

¹ *Notice of request for public comment on “Agency Information Collection Activities: Electronic Visa Update System,”* 82 Fed. Reg. 19,380 (Apr. 27, 2017) (hereafter “Notice”).

² Notice.

I. EPIC's Interest

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 the Department of Homeland Security (“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 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 changes⁷ 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[] media reports that reflect adversely on the U.S. Government [or] DHS”⁹ The DHS clearly intended to “capture

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/>.

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*, *New York Times*, Jan. 13, 2012, <http://www.nytimes.com/2012/01/14/us/federal-security-program-monitored-public-opinion.html>.

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.

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 EPIC submitted a statement for the record for that hearing opposing the agency’s media monitoring and called for the immediate end of the program.¹³ Members of Congress expressed concern about the federal agency’s plan to monitor social media.¹⁴

Given government misuse of social media monitoring techniques in the past, EPIC is skeptical of CBP’s proposal to use social media to scrutinize visa applicants during the vetting process. EPIC opposes this proposal.

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

CBP has stated that the agency will use the social media identifiers for “vetting purposes, as well as applicant contact information.”¹⁵ Little additional information is provided.

It is not clear how the CBP intends to use the social media identifiers. Other federal agencies have a history of using social media for controversial purposes. For example, DHS has

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).

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 Andrea Stone, *DHS Monitoring of Social Media Under Scrutiny by Lawmakers*, Huffington Post, Feb. 16, 2012, http://www.huffingtonpost.com/2012/02/16/dhs-monitoring-of-social-media_n_1282494.html; *Congress Grills Department of Homeland Security*, EPIC, Feb. 16, 2012, <https://epic.org/2012/02/congress-grills-department-of-.html>.

¹⁵ Notice.

monitored social and other media for dissent and criticism of the agency.¹⁶ Will the CBP 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 with? How will the CBP prevent Muslim and Arab Americans from being scrutinized more harshly?

Additionally, what information will the social media identifiers be combined with? Will CBP use the social media identifiers to obtain additional information about the applicant from social media companies? Will applicants be informed if the information obtained from their social media accounts led to the denial of their application? And does the acquisition of social media identifiers place at risk the privacy and security of account holders? Is CBP prepared to accept liability if the practice leads to identity theft or financial fraud?

Answers to these questions should be provided prior to adoption of CBP's proposal to acquire the social media identifiers of people suspected of no crime.

This proposal leaves the door open for abuse, mission creep, and the disproportionate targeting of Muslim and Arab Americans among other groups. This proposal is especially alarming in light of past misuses of social media from all levels of government¹⁷ as well as the

¹⁶ 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, <https://epic.org/privacy/socialmedia/EPIC-Stmt-DHS-Monitoring-FINAL.pdf>.

¹⁷ Elizabeth Dwozkin, *Police Are Spending Millions of Dollars to Monitor the Social Media of Protesters and Suspects*, Washington Post, Nov. 18, 2016, <https://www.washingtonpost.com/news/the-switch/wp/2016/11/18/police-are-spending-millions-to-monitor-the-social-media-of-protesters-and-suspects/>; *Map: Social Media Monitoring By Police Departments, Cities, and Counties*, Brennan Center for Justice, Nov. 16, 2016, <https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties>; Eric Yoder, *Beware What You Post: Federal Employees May Face Government Scrutiny on Social Media*, Washington Post, May 12, 2016, <https://www.washingtonpost.com/news/powerpost/wp/2016/05/12/beware-what-you-post-federal-employees-may-face-government-snooping-on-social-media/>.

Trump administration's controversial travel ban.¹⁸ CBP 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 prevent the targeting of individuals merely engaged in First Amendment protected activities.

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

CBP's proposal to collect social media identifiers of visa applicants also implicates the First Amendment and will have a chilling effect on protected speech. Freedom of speech and expression are core civil liberties and have been strongly protected by the Constitution and the U.S. courts.¹⁹ These rights extend to non-U.S. citizens.²⁰

Many people around the world use social media, including Facebook and Twitter, to support democratic movements and to campaign for political reform.²¹ But these political views reflect the specific circumstances of national political systems and regional political conflict, and there is some risk that comments taken out of context could discourage political reform efforts. For example, social media is credited with empowering the Arab Spring and allowing Egyptians

¹⁸ Alex Emmons, *Activists Worry That Social Media Vetting of Visa Applicants Could Quietly Expand Trump's Muslim Ban*, The Intercept, Mar. 23, 2017, <https://theintercept.com/2017/03/23/activists-worry-that-social-media-vetting-of-visa-applicants-could-quietly-expand-trumps-muslim-ban/>.

¹⁹ 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) (holding that immunity from state scrutiny of membership lists was related to the right of freedom of association and fell under the 14th Amendment of the U.S. Constitution); *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (holding that a city ordinance that required hotels to make their registries available to the police on demand was unconstitutional under the 4th Amendment of the U.S. Constitution).

²⁰ 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.").

²¹ Sophie Hutchinson, *Social media Plays Major Role In Turkey Protests*, BBC, Jun. 4, 2013, <http://www.bbc.com/news/world-europe-22772352>; David Auerbach, *The Bernie Bubble*, Slate, Feb. 17, 2016, http://www.slate.com/articles/technology/future_tense/2016/02/the_bernies_sanders_campaign_owes_a_lot_to_social_media.html.

to remove former President Hosni Mubarak from power.²² Social media also played a pivotal role in the 2013 Gezi Park protests in Turkey and the recent anti-Putin protests in Russia, which were sparked by a blog post and YouTube video.²³

CBP states that obtaining social media identifiers, presumably to view user accounts, will provide more information to be used in the vetting process.²⁴ However, the proposal assumes that social media provides an accurate picture of a person and those they are close with. People connect with others on social media for many 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 whether the social media accounts of U.S. citizens may be used as part of the vetting process.

The proposal also fails to explain how CBP will use social media as part of the vetting process. While the proposed question is intended to be optional, it is still a concern that CBP has failed to detail exactly how social media information will be used as part of the vetting process.²⁵ Many individuals have been on social media for years and have created a permanent record of their lives.²⁶ Teenagers are routinely warned to be careful of what they post on social media,²⁷

²² Amitava Kumar, *'Revolution 2.0': How Social Media Toppled A Dictator*, NPR, Feb. 8, 2012, <http://www.npr.org/2012/02/08/145470844/revolution-2-0-how-social-media-toppled-a-dictator>; Ramesh Srinivasan, *Taking Power Through Technology in the Arab Spring*, Al Jazeera, Oct. 26, 2012, <http://www.aljazeera.com/indepth/opinion/2012/09/2012919115344299848.html>.

²³ Steve Dorsey, *Turkey's Social Media And Smartphones Key To 'Occupy Gezi' Protests*, Huffington Post, Jun. 10, 2013, http://www.huffingtonpost.com/2013/06/09/turkey-social-media-smartphones-occupy-gezi-protests_n_3411542.html; Julia Ioffe, *What Russia's Latest Protests Mean for Putin*, The Atlantic, Mar. 27, 2017, <https://www.theatlantic.com/international/archive/2017/03/navalny-protests-russia-putin/520878/>.

²⁴ Notice.

²⁵ Notice.

²⁶ Alexandra Mateescu 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.

²⁷ 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>.

however teenagers and adults have made posts on social media which they later regret and may not be an actual reflection of who they are.²⁸ This 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 because of an inside joke or posturing that CBP does not understand from viewing certain information in isolation.²⁹ Furthermore, 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 Department 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 demonstrate a compelling interest that cannot be satisfied in other way.³⁰ Government programs that scrutinize online comments, dissent, and criticism for the purpose of vetting 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.

Concern over the how the government uses social media is widespread and several questions remain unanswered. Earlier this month, several members of the House of Representatives sent a letter to Attorney General Jeff Sessions raising concerns about how the

²⁸ 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/St8vHIqCLk7eRsvME3k5K/story.html>.

²⁹ Mateescu et. al., *Social Media Surveillance*; Brandon Giggs, *Teen failed for Facebook 'joke' is released*, CNN, Jul. 13, 2013 (discussing a teenager who was arrested after making a “threat” that, when viewed in context, appears to be sarcasm), <http://www.cnn.com/2013/07/12/tech/social-media/facebook-jailed-teen/>; 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>.

³⁰ See, e.g., *NAACP v. Button*, 83 S. Ct. 328 (1963); *Citizens United v. Fed. Election Comm'n*, 130 S. Ct. 876 (2010).

federal government and federal law enforcement agencies used technologies that monitored social media.³¹ Those Representatives noted how social media was effectively being used to monitor people who were suspected of no wrongdoing in violation of their Fourth Amendment rights stating:

There is evidence that social media data has been used to monitor protests and activists...An investigator at the Oregon Department of Justice used a service called DigitalStakeout to search Twitter for tweets using the hashtag #BlackLivesMatter. On the basis of his tweets – which included political cartoons and commentary but no indications of criminal activity or violence – the Department’s own Director of Civil Rights was deemed a “threat to public safety.”³²

The same concerns are present in CBP’s current proposal and these concerns must be addressed before any further steps are taken.

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.³³ 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 it leads to government profiling.³⁴ The availability of the SSN has been shown to contribute to identity theft and financial fraud.³⁵

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

³¹ Letter to Jeff Sessions from Keith Ellison et al., May 2, 2017, <https://www.documentcloud.org/documents/3696481-House-Democrats-Letter-to-Sessions-re-Social.html>.

³² *Id.*

³³ *Social Security Numbers*, EPIC, <https://epic.org/privacy/ssn/>.

³⁴ Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991). republished Marc Rotenberg, "The Use of the Social Security Number as a National Identifier," *Computers & Society*, vol. 22, nos. 2, 3, 4 (October 1991); Privacy Act of 1974, 5 U.S.C. §552a (2016).

³⁵ *Identity Theft*, EPIC, <https://epic.org/privacy/idtheft/>; *Social Security Numbers*, EPIC, <https://epic.org/privacy/ssn/>.

enhanced profiling and tracking of individuals. Furthermore, an individual has no way of knowing who in the government may be tracking them and for how long that surveillance could continue. What is initially presented as a way to vet visa applicants can turn into unwarranted, large scale surveillance of innocent people.

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. CBP has provided little transparency in how the agency plans to use social media identifiers collected from alien visitors. Such opaqueness in the CBP proposal provides little comfort that CBP will provide the transparency necessary to ensure that the program is subject to appropriate oversight and accountability.

EPIC urges CBP to withdraw its proposal to collect social media identifiers from visa applicants. Additionally, EPIC recommends that any current use of social media analysis by CBP 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 recommends that the CBP withdraw its proposal to collect social media identifiers. The proposal undermines privacy and is contrary to First Amendment rights of speech, expression, and association.

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott

Jeramie D. Scott
EPIC National Security Counsel

/s/ Kim Miller

Kim Miller
EPIC Policy Fellow