

BRENNAN  
CENTER  
FOR JUSTICE  
TWENTY  
YEARS

Brennan Center for Justice  
at New York University School of Law

161 Avenue of the Americas  
12th Floor  
New York, NY 10013  
646.292.8310 Fax 212.463.7308  
www.brennancenter.org

U.S. Customs and Border Protection  
Attn: Paperwork Reduction Act Officer, Regulations and Rulings  
Office of Trade  
90 K Street NE, 10th Floor  
Washington, DC 20229-1177

August 22, 2016

To whom it may concern:

On behalf of the Brennan Center for Justice at NYU Law School, we write to express our serious concerns about 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. The Brennan Center for Justice is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We regularly comment on matters related to national security and civil liberties, both in written comments and in testimony.<sup>1</sup> As described below, we believe that this policy is poorly conceived, fatally vague, apt to chill speech and reveal private information about travelers that is irrelevant to their suitability for entry to the United States, and likely to consume significant financial and personnel resources to produce little of value. The shortcomings in the policy fall into two main categories: unanswered questions, and substantive defects.

#### Unanswered questions

First, how is "social media" defined? The question proposed for addition to ESTA and Form I-94W says simply: "Please enter information associated with your online presence – Provider/Platform –

---

<sup>1</sup> See, e.g., *Willful Blindness: Consequences of Agency Efforts To Deemphasize Radical Islam in Combating Terrorism: Hearing before the Subcomm. on Oversight, Agency Action, Fed. Rights and Fed. Courts of the S. Comm. on the Judiciary*, 114th Cong. (2016), available at <https://www.brennancenter.org/sites/default/files/Mike%20German%20Testimony%20SJC%20Oversight%20Final.pdf> (written statement for the record submitted by Michael German, Fellow, Liberty and National Security Program, Brennan Ctr for Justice); Letter from the Brennan Ctr for Justice to the Privacy and Civil Liberties Oversight Board (June 16, 2015), available at <https://www.brennancenter.org/analysis/brennan-center-submits-comments-pclobs-12333-plan-1>; Memorandum from the Brennan Ctr for Justice to members of the Privacy and Civil Liberties Oversight Board (Oct. 26, 2012), available at <https://www.brennancenter.org/analysis/comments-submitted-privacy-and-civil-liberties-oversight-board>; *Ending Racial Profiling in America: Hearing Before the Subcomm. on the Constitution, Civil Rights and Human Rights of the S. Comm. on the Judiciary*, 112th Cong. (2012), available at [https://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/BrennanCenter\\_ERPA.pdf](https://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/BrennanCenter_ERPA.pdf) (written statement for the record submitted by Faiza Patel and Elizabeth Goitein, Co-Directors, Liberty and National Security Program, Brennan Ctr for Justice).

Social media identifier.” The term “online presence” is completely uncabined; there are no examples provided, and no language limiting the types of “providers” or “platforms” that should be included. Presumably, the department intends to include Facebook and Twitter. What about Instagram? Pinterest? Usernames for commenting on *New York Times* or *Wall Street Journal* articles? Aliases for interacting with other players in video games or Second Life? Amazon.com product reviews? These collectively make up an individual’s “online presence”; should the traveler provide information about all of them? The proposal provides no guidance.

Similarly, consider travelers who maintain multiple accounts on a single platform – perhaps a personal one and a professional one. If they share posting duties for a professional organization with multiple people, must they provide that profile information, and will they be held accountable for all posts on a particular profile over which they exercise only partial control? There are no limits to the type of information that could be encompassed by one’s “online presence” – and the more that is provided, the more intrusive and time-consuming the review process will be.

Second, when a traveler does choose to answer the question, what are the consequences for a perceived failure to answer correctly? The I-94W form requires applicants to certify that their answers are “true and correct to the best of my knowledge and belief.”<sup>2</sup> If an applicant chooses to provide information about certain social media accounts (for instance, a Twitter handle) but not others, whether by choice or inadvertent omission, will they be vulnerable to charges that the information they provided was not “true and correct” because it was not comprehensive? If so, will they be excluded from the country or face legal consequences?

Third, what authority will CBP officers have to demand information from travelers? The question states that it is optional, but will CBP officers be allowed to request social media information from travelers who have not already offered it, and if so, are the travelers obligated to provide it? If a traveler chooses to provide certain social media identifying information but a CBP officer believes it is not comprehensive, must the traveler provide additional information? The proposed policy sets out no guidance on this matter and invests individual officers with enormous power to elicit ostensibly voluntary information.

Finally, how are non-public accounts handled? For instance, if a traveler maintains a private Twitter account, such that only approved followers can see her tweets, is she obligated to accept a “follow” request from a CBP officer so the U.S. government may see her protected tweets? If a traveler has set strong privacy settings on his Facebook page, must he agree to be “friends” with a CBP officer, giving the officer access to years’ worth of personal postings, pictures, and more? If a traveler only has private accounts, will that in itself be seen as suspicious? The policy provides no direction on these matters.

Even assuming the department provides further guidance, however, significant problems with the substance of policy indicate that it should be shuttered before it is rolled out.

### Substantive problems

---

<sup>2</sup> *Form I-94W – Visa Waiver Arrival/Departure Record*, U.S. CUSTOMS & BORDER PROTECTION, <https://www.cbp.gov/document/forms/form-i-94w-visa-waiver-arrivaldeparture-record>.

First, this proposal finds its roots in a false narrative. Newspaper articles indicate that the policy – which had already been rejected once by the department – came into renewed prominence after the shootings in San Bernardino, CA, on December 2, 2015.<sup>3</sup> Early media reports in the immediate aftermath of the attack indicated that one of the shooters, Tashfeen Malik, had broadcast her intentions and her allegiance to the Islamic State on Facebook prior to entering the United States and prior to the attack.<sup>4</sup> Sen. Ted Cruz and others used this reporting to suggest that DHS had erred in not examining Malik’s social media accounts before allowing her to enter the United States and gain citizenship.<sup>5</sup> The reports were false, however, as FBI Director James Comey made clear two weeks after the attacks. In a December 16, 2015 statement, he said: “So far in this investigation we have found no evidence of the posting on social media by either of them at that period of time and thereafter reflecting their commitment to jihad or to martyrdom.”<sup>6</sup>

Second, the proposed question is unlikely to reveal information that will be genuinely useful in determining whether a traveler may safely enter the United States. To be sure, FBI Director James Comey and Homeland Secretary Jeh Johnson have spoken on multiple occasions about concerns that ISIS is recruiting through social media, and both the government and social media companies have already undertaken multiple initiatives to try to address this threat.<sup>7</sup> But it seems highly unlikely that an individual who promotes terrorism online will disclose information about the social media profile that he is using to do so. This lack of functionality raises the prospect that the form will instead be used to examine individuals’ political and religious beliefs as potential indicators of a propensity to terrorism, an approach that has no empirical foundation.<sup>8</sup>

---

<sup>3</sup> See Michelle Ye Hee Lee, *Ted Cruz’s False Claim the San Bernardino Shooter Posted Publicly on Social Media a Call to Jihad*, WASH. POST (March 26, 2016), <https://www.washingtonpost.com/news/fact-checker/wp/2016/03/26/ted-cruzs-false-claim-the-san-bernardino-shooter-posted-publicly-on-social-media-a-call-to-jihad/> (explaining false claims concerning social media policy); Ari Melber & Safia Samee Ali, *Exclusive: Homeland Security Passed on Plan to Vet Visa Applicants’ Social Media*, MSNBC (Dec. 17, 2015, 3:01 PM), <http://www.msnbc.com/msnbc/exclusive-homeland-security-rejected-plan-vet-visa-applicants-social-media> (explaining the Dep. of Homeland Sec. rejection of the previous plan).

<sup>4</sup> See, e.g., Matt Apuzzo et al., *U.S. Visa Process Missed San Bernardino Wife’s Online Zealotry*, N.Y. TIMES (Dec. 12, 2015), at A1, available at [http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html?\\_r=0](http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html?_r=0) (explaining that, “The original version of this article, based on accounts from law enforcement officials, reported that Tashfeen Malik had ‘talked openly on social media’ about her support for violent jihad.”).

<sup>5</sup> See Ye Hee Lee, *supra* note 3.

<sup>6</sup> Richard A. Serrano, *FBI Chief: San Bernardino Shooter Did Not Publicly Promote Jihad on Social Media*, L.A. TIMES (Dec. 16, 2015, 1:44PM) <http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html>.

<sup>7</sup> See, e.g., *Counterterrorism, Counterintelligence, and the Challenges of ‘Going Dark’: Hearing Before the S. Select Comm. on Intelligence*, 114<sup>th</sup> Cong. (2015), available at [https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2015/07/20/07-08-15\\_fbi\\_comey\\_testimony\\_re\\_counterterrorism\\_counterintelligence\\_and\\_the\\_challenges\\_of\\_going\\_dark.pdf](https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2015/07/20/07-08-15_fbi_comey_testimony_re_counterterrorism_counterintelligence_and_the_challenges_of_going_dark.pdf) (statement for the record of James Comey, Director, FBI) (“From a homeland perspective, it is ISIL’s widespread reach through the Internet and social media which is most concerning . . . . ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.”); *Worldwide Threats to the Homeland: ISIS and the New Wave of Terror: Hearing Before the H. Comm. on Homeland Sec.*, 114<sup>th</sup> Cong. (2016), available at <http://docs.house.gov/meetings/HM/HM00/20160714/105134/HHRG-114-HM00-Wstate-JohnsonJ-20160714.PDF> (written statement for the record submitted by Jeh Johnson, Secretary of Homeland Sec.) (“We have moved from a world of terrorist-directed attacks, to a world that also includes the threat of terrorist-inspired attacks – attacks by those who live among us in the homeland and self-radicalize, inspired by terrorist propaganda on the internet.”).

<sup>8</sup> FAIZA PATEL, *RETHINKING RADICALIZATION* (2011), available at <https://www.brennancenter.org/sites/default/files/legacy/RethinkingRadicalization.pdf>.

Third – and relatedly – problems of interpretation are guaranteed to plague any review of social media postings. One need only look at the 2012 experience of a British citizen who was turned back at the border because DHS agents were concerned about the traveler’s Twitter postings.<sup>9</sup> His offense? Saying that he was going to “destroy America” – slang for partying – and “dig up Marilyn Monroe’s grave” – a joke. One could imagine even greater difficulties with more subtle online expressions; what is DHS to do, for instance, with an applicant’s statement that “Of all the actors in the Syrian conflict, I don’t think ISIS is the worst”?

Moreover, the problem will become simply unmanageable in the context of the 38 Visa Waiver Program countries, many of which do not use English. Government agents and courts have erroneously interpreted tweets repeating American rap lyrics as threatening messages in several previous cases,<sup>10</sup> a problem that will only be exacerbated when they are asked to decode messages in Slovenian, Taiwanese, and Dutch.

This is to say nothing of the challenges posed by non-verbal communication on social media. Until recently, for instance, Facebook allowed only one kind of reaction to a post: a “like” symbol (or a comment). Recent updates allow users to react to a posting with emojis signaling “like,” “love,” “funny,” “wow,” “sad,” or “angry.”<sup>11</sup> The actual meaning of these emojis is still highly contextual, however. If a Facebook user posts an article about the FBI persuading young, isolated Muslims to make statements in support of ISIS,<sup>12</sup> and another user “loves” the article, what does that mean? Is he sending appreciation that the article was posted, signaling support for the FBI’s practices, or sending love to a friend whose family has been affected? Or some combination of the above? Assuming it is even possible to decode the meaning, it could not be done without delving further into the user’s other online statements, interactions, and associations, as well as the postings of those with whom he or she communicates, a laborious, invasive, and error-riddled process. Indeed, such ambiguity is already affecting domestic criminal proceedings, with dire consequences.<sup>13</sup>

Similarly, Twitter recently replaced its “favorite” button (a star) with a “like” button (a heart).<sup>14</sup> This posed a dilemma for many users of the popular platform, who had used the star button to mark a

---

<sup>9</sup> See J. David Goodman, *Travelers Say They Were Denied Entry to U.S. for Twitter Jokes*, N.Y. TIMES: THE LEDE (Jan. 30, 2012, 1:03 PM), [http://thelede.blogs.nytimes.com/2012/01/30/travelers-say-they-were-denied-entry-to-u-s-for-twitter-jokes/?\\_r=2](http://thelede.blogs.nytimes.com/2012/01/30/travelers-say-they-were-denied-entry-to-u-s-for-twitter-jokes/?_r=2).

<sup>10</sup> See, e.g., Natasha Lennard, *The Way Dzhokhar Tsarnaev’s Tweets Are Being Used in the Boston Bombing Trial Is Very Dangerous*, FUSION (March 12, 2015), <http://fusion.net/story/102297/the-use-of-dzhokhar-tsarnaevs-tweets-in-the-boston-bombing-trial-is-very-dangerous/>; Bill Chappell, *Supreme Court Tosses Out Man’s Conviction for Making Threat on Facebook*, NPR (June 1, 2015), <http://www.npr.org/sections/thetwo-way/2015/06/01/411213431/supreme-court-tosses-out-man-s-conviction-for-making-threats-on-facebook>.

<sup>11</sup> See Sammi Krug, *Reactions Now Available Globally*, FACEBOOK NEWSROOM (Feb. 24, 2016), <http://newsroom.fb.com/news/2016/02/reactions-now-available-globally/>.

<sup>12</sup> See, e.g., Eric Lichtblau, *F.B.I. Steps Up Use of Stings in ISIS Cases*, N.Y. TIMES (June 7, 2016), <http://www.nytimes.com/2016/06/08/us/fbi-isis-terrorism-stings.html> (“In recent investigations from Florida to California, agents have helped people suspected of being extremists acquire weapons, scope out bombing targets and find the best routes to Syria to join the Islamic State, records show.”); Murtaza Hussain, *Confidential Informant Played Key Role in FBI Foiling Its Own Terror Plot*, INTERCEPT (Feb. 25, 2015, 9:09PM), <https://theintercept.com/2015/02/25/isis-material-support-plot-involved-confidential-informant/> (explaining that, “[N]one of the three [conspirators] was in any condition to travel or support the Islamic State, without help from the FBI informant.”).

<sup>13</sup> See, e.g., Ben Popper, *How the NYPD Is Using Social Media to Put Harlem Teens Behind Bars*, THE VERGE (Dec. 10, 2014), <http://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison>.

<sup>14</sup> Robinson Meyer, *Twitter Unfaves Itself*, THE ATLANTIC (Nov. 3, 2015), <http://www.theatlantic.com/technology/archive/2015/11/twitter-unfaves-itself-hearts/413917/>.

post for later review or signal its relevance without taking a position on the content: would they now “heart” tweets with which they vehemently disagree? If they did “heart” a tweet, does that signal to the writer and to the user’s followers that they are in accord with the sentiment? More urgently for these purposes, what does it signal to the U.S. government?

This may be an especially serious issue for journalists, particularly those writing on conflict zones: when a foreign journalist “hearts” a provocative tweet from an ISIS follower to be able to find it again more easily for a piece of writing, will that be taken as support for the follower’s positions? And will he or she then be called to account for every “heart” and “like”? Political scientists and other scholars will face similar quandaries. In light of the multitude of possible interpretations of both speech and non-verbal communication, DHS will be able to exercise enormous, unchecked discretion when it comes to allowing travelers and immigrants into the country and quizzing them about the meaning and significance of a range of expression.

In addition, protected speech, particularly of the political or religious variety which might raise red flags with U.S. officials, will inevitably be chilled. As travelers become aware of the DHS’s request for information – and certainly if the request becomes either a *de facto* or a *de jure* demand instead – many will surely sanitize their own postings and Internet presence to ensure that nothing online would provide cause for further scrutiny or suspicion by a rushed CBP officer. Even if these travelers do not have First Amendment rights, a system that penalizes people for statements they make online, simply because they are susceptible to misinterpretation, is profoundly incompatible with core American constitutional values. It is also incongruent with the Universal Declaration of Human Rights, which guarantees “the right to freedom of opinion and expression,” including the “freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”<sup>15</sup>

Fourth, reviews of travelers’ social media profiles will also likely reveal other personal information, including their connections to friends, relatives, and business associates in the U.S., potentially subjecting Americans to invasive scrutiny of their personal lives via an unregulated and secret program.

Finally, this deeply flawed policy comes at a steep cost to the American taxpayer: approximately \$300 million per year, by DHS’s own estimate.<sup>16</sup> This cost is far too high for the scant gains that the program can be expected to produce and the myriad problems that it will generate. Accordingly, we urge DHS to abandon this proposal at the outset.

Please do not hesitate to let us know if we can provide any further information regarding our concerns. We may be reached at [faiza.patel@nyu.edu](mailto:faiza.patel@nyu.edu) (Faiza Patel: 646-292-8325) or [rachel.levinson.waldman@nyu.edu](mailto:rachel.levinson.waldman@nyu.edu) (Rachel Levinson-Waldman: 202-249-7193).

---

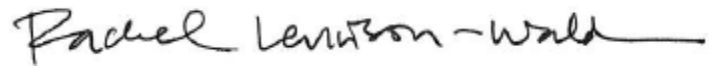
<sup>15</sup> Universal Declaration of Human Rights, G.A. Res. 217A (III), Article 19, U.N. Doc. A/810 at 71 (1948), <http://www.un.org/en/universal-declaration-human-rights/>.

<sup>16</sup> See Agency Information Collection Activities: Arrival and Departure Record (Forms I–94 and I–94W) and Electronic System for Travel Authorization, 81 Fed. Reg. 40,892 (June 23, 2016), at 40,893, *available at* <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#p-16> (estimating cost burden of various aspects of the program).

Sincerely,

A handwritten signature in black ink, appearing to be 'Faiza Patel', with a stylized, cursive script.

Faiza Patel  
Co-Director, Liberty and National Security Program

A handwritten signature in black ink, appearing to be 'Rachel Levinson-Waldman', with a cursive script.

Rachel Levinson-Waldman  
Senior Counsel, Liberty and National Security Program