

Comment Submitted by David Crawley

**Comment**

View document:

The notion that my social media identifier should have anything to do with entering the country is a shockingly Nazi like rule. The only thing that this could facilitate anyway is trial by association - something that is known to ensnare innocent people, and not work. What is more this type of thing is repugnant to a free society. The fact that it is optional doesn't help - as we know that this "optional" thing will soon become not-optional. If your intent was to keep it optional - why even bother?

Most importantly the rules that we adopt will tend to get adopted by other countries and frankly I don't trust China, India, Turkey or even France all countries that I regularly travel to from the US with this information.

We instead should be a beacon for freedom - and we fail in our duty when we try this sort of thing.

Asking for social media identifier should not be allowed here or anywhere.

Comment Submitted by David Cain

**Comment**

View document:

I am firmly OPPOSED to the inclusion of a request - even a voluntary one - for social media profiles on the I-94 form.

The government should NOT be allowed to dip into users' social media activity, absent probable cause to suspect a crime has been committed.

Bad actors are not likely to honor the request. Honest citizens are likely to fill it in out of inertia.

This means that the pool of data that is built and retained will serve as a fishing pond for a government looking to control and exploit regular citizens.

An authoritarian government (for which we're at risk this election cycle) could easily abuse this information, and the networking/contact information it enables.

Since government is regularly augmenting its security practice with private contractors, this information will also be available to those contractors, who may attempt to monetize information on private citizens as well, without explicit consent.

Government does not delete acquired data without a requirement to do so, so this data, once collected, has an indefinite life, much longer than any proximate concern around cross-border travel.

Further, the linking of traveler name and social media account destroys anonymity, for social media users who may be victims of domestic violence, whistle-blowers, confidential media sources, community organizers, or others with a need for anonymity.

Finally, "optional requests" for information have a way of becoming requirements for information, through the expansion of government power that we've seen since 9/11, through inaction of people

who could stop this, or through simple bureaucratic or programmer error.  
Please reject this change to I-94.

Comment Submitted by Peio Powieur

**Comment**

View document:

The proposal to ask applicants for social media information in Form I-94W is complete nonsensical. The proposal reflects:

- (a) a shockingly naive belief that travelers who are threats are of sufficiently low intelligence to provide authentic social media identifiers,
- (b) a disturbingly naive view that social media are a statistically valid and scientifically reliable source of information about anything,
- (c) a lack of concern for the invasion of innocent travelers' privacy counter to accepted and universal human rights principles,
- (d) a complete disregard for the effective use of taxpayer funds and government staff resources (following from the previous points), and
- (e) a complete lack of discussion about how the requested social media information will be used, how it will be kept secure, how long it will be retained, how it will be shared with other agencies, etc.

I urge CBP to drop this ridiculous proposal and focus its resources on information sources and procedures that actually support thoughtful and accurate analysis and are respectful of travelers' privacy and security.

Comment Submitted by Anonymous

**Comment**

View document:

Adding an optional data field to request social media identifiers:

1. Invades the privacy of tourists who want to visit the USA without any benefit to security.
2. Since it's optional (so far) I suspect most will not provide social media identifiers. I wouldn't even if I had such identifiers.
3. It encourages other countries to implement similar rules, in retaliation, for US citizens visiting those countries.

Do not implement these new rules.

Comment Submitted by Anonymous (Concerned Citizen)

**Comment**

View document:

I am in direct and absolute opposition to this latest invasion of privacy. It doesn't matter if I have "nothing to hide" or that it "doesn't affect me". This is a deliberate step towards a complete police state in this country. I will fight this tooth and nail, with every resource at my disposal, and so will every free thinking citizen.

Comment Submitted by Bin Li

**Comment**

View document:

Good idea! Also suggest to check the website [www.wenxuecity.com](http://www.wenxuecity.com), you will find a lot of anti-America Chinese living in the US. They need to be sent back home if they hate America and American values so much.

Comment Submitted by Larry Menard

**Comment**

View document:

I hope you make it mandatory. That should keep out a few undesirables.

Comment Submitted by Anonymous (German Traveller)

**Comment**

View document:

I am officially protesting against this new invasion of privacy which will yield no useful data but contributes to the ongoing madness of collecting data wherever whenever possible - with no RELIABLE information about how long the data will be stored or who else it will be related to.

Comment Submitted by Randy Bush

**Comment**

View document:

This is overly invasive of privacy and will yield no useful data.

Comment Submitted by Tom Brover

**Comment**

View document:

If this was in effect, I would refuse to hand over my social media information or hand over false handles.

Comment Submitted by Anonymous

**Comment**

View document:

Dear C.B.P.

Regarding your proposal to include social media "identifiers" as part of ESTA online application.

This is ludicrous and an unnecessary and non-essential intrusion into privacy, not to mention a waste of human plus material resources (paper or otherwise). It has the potential to create unnecessary lists of thousands (or hundreds of thousands) of 'persons of interest' that need to be 'vetted'. As if we don't have enough unnecessary surveillance already.

If the relevant U.S. enforcement and intelligence agencies were communicating and sharing more information between each other, I doubt we would need to hear of this proposal. Even if it is proposed to make this an 'optional' question, what assurance do we have from DHS or Congress that declining to answer this question will not prejudice an ESTA application? None.

Last year, Facebook and Google officials reportedly questioned the U.S. government over the need for U.S. intelligence or enforcement agencies to pierce their encryption technology, suggesting it could lead to less accountability from law enforcement officials.

Earlier this year there it was reported in the news of a suggestion from U.S. government to use "algorithms" on social media to try and detect terrorist content online. I do not think data mining is not the magic wand that will help here. A lot of false positives and unnecessary anguish could easily be generated from erroneously targeting what might be falsely perceived as potential offenders.

Ditch this idea, DHS and Congress, and find more resourceful ways of utilizing existing resources.

Comment Submitted by Matthew [Last Name Unknown]

**Comment**

View document:

The scope of social media is unconstrained, which poses issues related to excessive government oversight, government accessibility of data, and feasibility of search. Starting with accessibility, many parts of modern social media are not publically available, or intentionally temporary, making it impossible for US customs to access, either technologically, or without forcing a hosting provider to give up access, which would likely lead to protests on the grounds of the Fourth Amendment. Even without existing court precedent, this type of search violates the spirit of the Fourth Amendment by "collecting social media data" that was intended to be private, as indicated by privacy settings/social media platform expectations. Without coercing access to private areas, it is likely an unhelpful tool for finding any potentially nefarious activity. Continuing to feasibility, it is unlikely to be feasible for a hand search of any social media accounts, so it is assumed any searches are most likely automated. This presents an issue as there are many different social platforms which use proprietary interfaces that would require custom software to search. This makes it impossible to cover all platforms reducing efficacy of data collected, and potentially increasing costs. Thus my primary concerns are related to A and E, in that customs cannot practically access the data, making the collection useless and/or ethically and potentially legally problematic, and also in its implementation likely being very expensive in attempts to actually collect/use the data.

Although this legislation has no direct impact to me as an existing US citizen, I value privacy, and believe US customs processes are used as a model internationally, which would then affect me as I travel abroad. Dropping the addition of the social media field and keeping ESTA/I-94W the same is my proposed solution. Thank you for considering concerns that the public has on this topic.

Jonathan Corbett  
382 NE 191<sup>st</sup> St. #86952  
Miami, FL 33179  
June 29<sup>th</sup>, 2016

To: 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.

Re: **Request for Comments - Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization (81 FR 40892)**

To Whom It May Concern:

I am a civil rights advocate specializing in travel-related privacy issues. As a U.S. citizen, I will never have to file an "ESTA," but I have 4 concerns regarding the proposal that are the basis for this **opposition** to the proposed rule:

1. **The rule will be ineffective for its stated purpose.** By introducing a field to optionally specify social media accounts, you are accomplishing nothing. According to the proposed rule, someone with criminal intent related to their entry into this country can simply fail to answer this question without penalty. Asking this question is about as effective as pornographic Web sites asking their visitors to "confirm" that they are over the age of 18 is at stopping teenage boys from looking at naked women. Further, I find it likely that your true intent is to introduce this change as "optional" such that it meets less opposition, and then change it to "mandatory" in the near future, much like the TSA just did with its nude body scanners. See "Passenger Screening Using Advanced Imaging Technology," 81 FR 11363.
2. **The rule is a burdensome invasion of privacy.** Quite frankly, the government has no business asking tourists to disclose their social media accounts. Nowadays, people use social media to communicate with their friends, family, and business contacts, and such information is highly personal. Absent suspicion, our government should not be asking

for this data. Further, by failing to define “social media” or put any boundaries on what information the government seeks to collect, travelers who wish to answer this question may be unclear as to what qualifies. Do I need to think back to the MySpace account that I created in 2003 and have not used since 2006? If I have a username for a chat room or message board, does that count? What about Tinder? Or perhaps I use the popular dating app for gay men known as Grindr. Do you think it’s reasonable that I would then need to indirectly disclose my sexual preference as a condition of entering this country? Or perhaps I use the Web site for connecting individuals with sexual fetishes known as FetLife. Will you then review my FetLife account and determine if my preferred variety of kinky sex is acceptable? If it is uncovered that I enjoy being dominated by women in latex bodysuits while ball gagged, will a CBP officer consider me the same level of security risk as one who prefers long walks on the beach and seeks a partner who loves Jesus? Speaking of Jesus, many people use social networking related to their religion (Christian Mingle, JDate, etc.). Now you’d like to know my religion, too?

3. **The rule does not specify how the data will be retained and used.** As I’m sure you are aware, the federal Privacy Act places significant burdens on government agencies that wish to collect or retain data. Until the government can identify *with specificity* how the data will be stored and how it will be used, it should not be collected. (A half-assed explanation that the data collection will provide “greater clarity and visibility” does not explain *with specificity*.)
4. **The rule will subject U.S. citizen-travelers to retaliation.** When the U.S. government implements a stupid rule affecting foreign visitors, other countries implement retaliatory rules on U.S. citizens seeking to enter their territory. The first instance of this was perhaps the U.S.-Canada border, which is now quite needlessly more difficult to cross than our border with Mexico, after U.S. authorities started demanding criminal record data from the Canadian government for the purpose of prohibiting Canadians with minor criminal convictions from entering. Now, a U.S. citizen cannot enter Canada if he is, for example,

convicted within the last 10 years of driving with a blood alcohol level of 0.05% -- a petty misdemeanor in every jurisdiction in the country that penalizes that level of "intoxication." Many other countries require visa fees only from U.S. citizens (or higher visa fees only for U.S. citizens), or fingerprinting only for U.S. citizens, in retaliation for what we do to their citizens. I don't want to have to share my Facebook details in order to travel, and if you implement this rule, it is all but certain that I shall have to do so as other countries decide to implement retaliatory rules.

Instead of coming up with useless rules that will burden both foreigners and U.S. citizens alike, why not work on doing things that will actually and easily protect the homeland, like securing our border with Mexico? (For the record, I'm not particularly concerned with the Mexican families who sneak across the border to build a better life for their children, but I *am* concerned that if an impoverished family of 4 can do it, a well-funded terrorist could do the same.)

Thank you very much for your time – I understand it is burdensome to have to file all of these comments before ignoring them and doing exactly what you planned to do anyway.

Sincerely,

Jonathan Corbett

## Comment Submitted by Carrie- Ann M. Tooley

### Comment

View document:

What I am seeing is, like many other Americans in-service to the public, these people are already over-worked. In-fact, the US Customs and Border Patrol website says that in 2012 alone, Border Patrol agents made over 364,000 arrests of people illegally entering the country. That is approximately 100 people arrested per day. If this number is accurate, this is an incredible feat. And from the outside looking in, it looks as though we're trying to give these people even more to do instead of considering other solutions. It reminds of a form of micromanaging - giving more and more work, taking away more and more self-ownership, and expecting results without ever having walked in the shoes of the one's that we're making decisions for.

I propose that we ask the Border Control agents what their perspective on this is. And not the administration - the actual workers. Do they see that monitoring Social Media is the best or most effective use of their time?

Additionally, there are some other points that require looking at.

First, everything is already known - everything that we do on the internet is stored and accessible. So, creating this idea that it's not is very strange. Perhaps it is time to make the public aware of this and to make clear to citizens that they need to stop doing whatever it is that they believe is and/or must be kept secret or private - else they compromise themselves, their integrity, and each other. We need to expect more from our fellow human beings and stop going into the idea that they are 'just human'.

Next, we have some real problems with human trafficking, drugs, and illegal immigration. Despite the efforts of our hardworking Law Enforcement, Drug Enforcement, Border Control, and Homeland Security workers, the problems are not improving - they are getting worse. Why is it that we haven't figured out, like Carl G. Jung said, that "What you resist, persists?" - where, for each one of these criminals that



are arrested, a few more will come to take their place. And within this, how it continues on and on and on. It makes one question: have those in positions of making the decisions to add more control aware of this? Are they seeing what we are seeing? Do they need better support and assistance from those of us who are seeing the patterns repeating and compressing?

In sum, this proposal makes very little sense when looking at the big picture. Instead of creating a reaction in people, we need to be upfront with them and start educating them. We're all in the same boat here and have been living in an extensive amount of stress for many years - why perpetuate it or add to it? And further, why make it look like our 'good guys' are the enemy that's set out to take away some apparent privacy? Enough is enough. Really.

Thanks for your time.

Warmest Regards,

Carrie Tooley

-----  
Comment Submitted by Seth Uhl

Comment

View document:

Its fine

-----  
Comment Submitted by Justin Collins

Comment

View document:

I am opposed to this addition.

I fail to see how this would help keep anyone safe. If someone has suspicious activity on the social media accounts, they can just not answer this optional field. For everyone who honestly answers, it provides more government monitoring of their personal lives and more opportunity for identity theft.

The \$265 million price tag is not justifiable.

-----  
Comment Submitted by G .Fox

Comment

View document:

Those decrying this proposal as a GOVERNMENT intrusion into their privacy are missing the point; YOU gave that up to social media long ago, and the dots are out there to be connected. The USCBP is just trying to cover their butts against admitting someone who openly declared death to America -- can't fault them for that.

It's still an ineffective proposal, though, and I'd like to register my complaint against it on the grounds it normalizes social media and its attendant erosion of the entire notion of privacy. (Or modesty, or decorum, or literacy, etc.).

Generally: I understand the USCBP can't intercept every adversary, and I'll take liberty over security. Thank you!

-----  
Comment Submitted by Kevin Murphy

Comment

View document:

Hello,

I object to the proposal to modify Form I-94W to request information associated with online presence providers / platforms / social media identifiers.

Firstly, there are no privacy and data handling provisions associated with how the collected information will be used, and when (or if) it will be destroyed. Any collection of information should clearly state this in a policy, but that policy is not on the form. It took me, an experienced IT professional, fifteen (15) minutes to locate the I-94 form privacy information on the CBP website. Turns out, this information will be retained for at least

seventy-five (75) YEARS.

Secondly, the collection of this information is disingenuous. It will allow linkages to be created between a person's identity issued by a government (passport numbers), physical address, and online personas. This is a dangerous level of linkage about a person. The government parties that this information will be shared with don't have great controls over use (or mis-use) of this type of information.

Thirdly, by creating this data source, an attractive source of information is created for other governments to attack. Who wouldn't want a database that links everybody's physical identity with their online identity? I'm sure the FBI and CIA would like this info, but so do a lot of other governments.

Finally, the rule change has not presented a necessary need for this information. It's even an "optional" field - not required. If we don't need it, then don't collect it. It's the core principal of data privacy - don't collect what you don't need.

Please don't approve this rule change.

-----

Comment Submitted by William Hargreaves

Comment

View document:

I am an occasional tourist to the United States from the United Kingdom. I like the ESTA system because it seems to make the process of entering the United States quicker than it would otherwise be. I cannot comment on the need for requesting social media information from travellers, as, like other contributors whose comments I have seen, I am not an expert in such matters.

Unlike other contributors, I think Social Media information, if required, would only work if it were compulsory. How you can ascertain whether people use social media is not my concern. My concern is that people like me, whose comments on social media are outspoken but in no way genuine subversive, or supportive of illegal acts, will happily share my information.

Unfortunately I suspect that those plotting crime against the United States are unlikely to provide details of their real Social Media interactions voluntarily if they have something to hide.

So, in summary, I am not sure how feasible, cost-effective and realistic it is to spend the money and time checking millions of online accounts each year, but if it is to be done, I suspect it might have to be compulsory. Otherwise it would not include information about people who are reluctant to provide the information (unless refusing to provide information would of itself be part of profiling a person as un-co-operative and under suspicion.

-----

Comment Submitted by Chris [Last Name Unknown]

Comment

View document:

I'm strongly opposed to the inclusion of a line asking about the social media IDs of people. This is way out of what the government needs to know for allowing somebody the permission to visit USA. It's an invasion of privacy and people's rights.

---

-----  
Comment Submitted by Scott Francis

Comment

View document:

Re: Proposed Changes to CBP Forms I-94, I-94W

Title: Arrival and Departure Record, Nonimmigrant Visa Waiver Arrival/Departure, and Electronic System for Travel Authorization (ESTA).

OMB Number: 1651-0111.

Form Numbers: I-94 and I-94W.

The proposed rule changes are ill-advised and should not be implemented, for several reasons:

1) those actually intending harm or malice (or who are simply uncomfortable with what's being requested) can simply opt not to provide the requested information, or can provide fictitious or incomplete information - as long as this is optional, it is pointless as a vetting method;

2) there's no way to make this requirement mandatory, as many applicants will not have any social media accounts to provide (or will have accounts with one of hundreds of varying providers with varying degrees of access or records retention, located in jurisdictions around the globe);

3) there's no way to confirm authenticity or completeness of the provided information (if any) - entirely legitimate (or fictitious) accounts could be submitted that do not represent the totality of a person's online identity.

Given that it is completely impossible to assure the quality, accuracy or comprehensiveness of the proposed data to be collected, attempting to do so is a waste of time and money that contributes no useful information to the vetting process. Indeed, the proposed changes merely further cloud the vetting process with inconsistent and entirely arbitrary information that cannot (by definition) be relied upon for any value at all.

In conclusion: adding to the hay to the stack does not improve one's chances of finding the needles.

-----

Comment Submitted by Rebecca Janzen

Comment

View document:

I am strongly opposed to the requirement to supply social media information before entering the US. It is an unnecessary invasion of privacy and may increase the risk of identity theft. I do not believe that it will enhance national security at all, certainly not enough to justify the added expense and the added indignity inflicted upon visitors to your nation.

-----

Comment Submitted by Liro Auterinen

Comment

View document:

Collecting data on people's online presence with details about their Social media identifier at different internet Providers and Platforms is an overkill in hunting terrorists and violates people's rights for privacy and freedom of opinion. It is the same than asking peoples political opinions, memberships in political parties or citizen's movements, sexual orientation etc.

Filling out the multiple questions of the Electronic System for Travel Authorization (ESTA) system is already now a time consuming burden for foreigners entering US within the Visa Waiver Program; it takes nearly an hour to fill if you really pay attention to all the long texts and your answers.

To propose an additional requirement with a time burden estimate of 23 minutes is presumptuous:

Electronic System for Travel Authorization (ESTA):

Estimated Number of Respondents: 23,010,000.

Estimated Time per Response: 23 minutes.

Estimated Total Annual Burden Hours: 8,812,830.

Estimated Annual Cost to the Public: \$265,020,000

-----  
Comment Submitted by Russell Neches

**Comment**

View document:

The only justifiable reason to conduct a search of a traveler's social media accounts is if there is already probable cause to suspect a violation or planned violation of the relevant US laws. It would only be appropriate to request access to the traveler's social media accounts AFTER initiating a more thorough examination.

For example, if Customs agents suspected that a person might be attempting to enter the United States under an assumed identity, it would be reasonable to compare the documents submitted to the relevant social media accounts (for example, to make sure the names and photographs all appear to belong to the same person). If there were probable cause to suspect that someone was seeking entry into the United States with the intention of harming another person -- to harass an ex-girlfriend, for example -- it would be reasonable to examine the traveler's social media posts to see if they contained menacing language.

It would not be reasonable, nor ethical, nor lawful, to examine someone's social media presence without probable cause, or having done so, to take action based on speech that is protected by the Constitution. For example, suppose a search is conducted because there was reason to suspect the traveler of seeking entry under an assumed identity; speech of a political nature, however distasteful to the agent, must to be considered irrelevant.

Moreover, if a search conducted on the basis of probable cause yielded speech of a questionable nature -- say, a selfie of the subject smoking pot -- it should not be deemed pertinent to the person's intent regarding their behavior while in the United States.

Any policy for examining social media should be based on the principle that information gleaned is of suspect veracity. It should be ASSUMED that there is likely to be deliberate manipulation, both favorable and unfavorable, of that person's presentation on social media. It must be TAKEN AS A GIVEN that the subject manipulates their own presentation (as is their right), but also that third parties may also manipulate their presentation. Third parties may have malicious intent towards the subject, or towards the United States, or towards both, but the subject has no control whatsoever over the actions of third parties. Moreover, it is difficult (and sometimes impossible) to clearly distinguish aspects of social media data are attributable to the subject or to third parties.

Everyone has someone in their family who posts embarrassing political nonsense on Facebook. Suppose a young Muslim man is seeking entry into the United States, and there is an inconsistency in the spelling of his name between his passport and his plane ticket. A search of his social media presence is conducted to verify that he is who he claims to be, and it is discovered that he is being honest about his identity. However, it is also discovered that there are posts on his Facebook timeline from his uncle that advocate violence against Americans. What, if anything, are we to make of this?

Any sane policy must result in setting aside the uncle's online rants. Otherwise, who among us does not have at least one family member whose political rants could land us in hot water? Or a coworker? Who among us does not have a single ex-girlfriend or boyfriend who would find it amusing to get us in trouble?

It does not strike me as wise policy to make United States Customs and Border Protection agents into clueless participants in the family drama, workplace politics and romantic lives of every traveler. It is an unfair expectation to place on agents that they ought to impartially adjudicate the intent behind this kind of personal information.

However, AFTER the traveler has been admitted into the United States, I think it would be a lovely idea for the government to offer to use social media to make their stay safer and more pleasant. The government should offer to use social media to warn tourists about emergencies, scams and bad weather in the areas they are visiting. The government should offer advice about places they are visiting ("Oh, it looks like you're heading to San Francisco! Since this is your first time visiting, you should know it's probably colder than you might expect. Don't forget a sweater!"). The government should offer to remind people about any important official deadlines that affect them ("Your visa is valid for another seven days. If you need to stay longer, here are some links to the rules that apply to you.").

As an American, I *\*WANT\** people from overseas to come here. I want them to spend money, have a good time, and learn about our culture. I want them to go home happy, to tell their friends and family what a wonderful time they had, and to visit again. The government definitely should be using social media to make coming to America a safe, affordable and enjoyable experience.

-----  
Comment Submitted by Eric Donahue

**Comment**

View document:

This is the most flagrant violation of our constitutional rights to privacy I have ever seen, worse even than the PATRIOT Act. Social media accounts are not meant to be a form of official government identification and never will be--including this on the I94W is tantamount to requiring citizens to list all the magazines they subscribe to, the bumper stickers they've put on their cars, which journalists they know, or which religious decorations they display over the holidays. Whatever illusion of safety is granted by the spying powers this would enable is absolutely, resolutely outweighed by the chilling creation of a sprawling, secretive federal database of OFFICIAL digital profiles of American citizens' private lives.

-----  
Comment Submitted by Roelin Polan

**Comment**

View document:

This should not be an acceptable form of information to collect from people arriving or departing from the US. Simply put, social media is a part of someone private thoughts and beliefs and is not a reasonable thing for the government to ask them to hand over. I understand it is not access but the affiliation to the account, but even then it is not fair to judge a person based on an Internet account. Given the recent trend in cyber warfare against innocent users by malicious hackers it is difficult to ever know if something is posted by the account that actually belongs to the user or to some hacker. Therefore judging their state based on things the account posts is not an accurate measure to know if a person is suspicious.

*No documents available.*

**Attachments**

View All (0)

---

Comment Submitted by Marisa Castillo

**Comment**

View document:

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

I do not believe that asking people for access to their social media accounts is a legitimate way to screen people coming into or leaving the United States of America. The question itself is problematic. What constitutes social media? Such a broad use of the word could open up a wide verity of platforms that are frankly none of the governments business.

Bad guys aren't going to post their evil deeds on public platforms. This is nonsense. And although it may appear optional a foreign traveler may feel pressured to release these details that are irrelevant to their traveling itinerary.

It is incredibly easy to create a narrative of what is going on in someone's personal media accounts when really that is not at all what is going on. We see this daily at the supermarket checkout line. Celebrity magazines and Gossip Rags creating these false narratives to sell magazines and make money. If the paparazzi can do it, how easily could government officials create a story to match whatever agenda they are trying to achieve.

And not only does it affect the privacy of the individual it affects the privacy of the people in that individuals circle of family and friends; more personal details that the government has no right or need to.

Certain types of public media cater to specific cultural, religious, or racial groups. This would affect the evaluation of certain groups of people disproportionately.

It would limit the types of speech we are free to place on our social media sites for fear of how it could affect us when traveling. It's giving permission to the government to monitor us. That doesn't sound very American. It sounds Orwellian. It would sensor the person's online speech and that is not what being an American is about. The United States of America is about sharing our thoughts and feelings without the fear of the government spying, evaluating, and retaliating against us.

I believe adding this question to the screening process will only cause more paperwork (which perhaps violates the Paperwork Reduction Act of 1995) and take more time to review and will only delay an already rigorous screening process that already does a very good job of screening visitors. I believe that it would only be a gateway to the continuation of these types of surveillance requests that are constantly trying to creep into our daily lives. It is a violation of privacy and I cannot support the government or any agency having access to anyone's social media accounts. I would not want my tax money going towards developing this line of questioning. I believe it is a waste of my tax money. I do not support it.

Thank you.

---

Comment Submitted by Linda Sherry

**Comment**

View document:

Re: Arrival and Departure Record, Nonimmigrant Visa Waiver Arrival/Departure, and Electronic System for Travel Authorization (ESTA). OMB Number: 1651-0111. Form Numbers: I-94 and I-94W.

Dear sir or madam,



This is absurd to ask, even optionally, for entrants' social media account identifiers. I see no reason why people should be asked to volunteer this information and many unsophisticated people will do so voluntarily, not realizing that their names and passport numbers will be associated with their social media presence in the databases of the federal government. If DHS needs to investigate someone with probable cause they can get court approval to find this information out. To simply troll for this information on a form that must be passed out to all entrants is an invasion of fundamental privacy rights. Perhaps many people have their social media accounts set to be easily findable, but many, many others guard this information closely and share it only with friends and family. Please retract this bad idea.

---

Comment Submitted by Asia Sias

**Comment**

View document:

This plan clearly infringes on our freedom of speech rights, as well as our privacy. First of all, being an optional choice, consent will likely only be given by those who feel pressured to fill in the entire form, or who do not understand what is being done with the information. This is not a valid way to find criminals. Second, those who consent to this are also signing up whomever might have spoken with them via the social media platform, infringing on their rights without their consent.

Lastly, this plan has no clear substance in regards to how it will help. What will be considered a threat? Which social media platforms will be investigated? How far back will the CBP be looking?

If this plan goes into effect, social media will no longer be a place of freedom, as we will have to regulate our opinions in order to not be considered suspicious. This plan should not be executed.

---

Comment Submitted by Martin Buss

**Comment**

View document:

So, what happens to visitors that DONT HAVE social media accounts? Not everyone has them! There are some no technical people that don't use them, and some people that see them as a risk to their private lives and information....up until now i thought such people were paranoid. now i am beginning to think maybe they are smarter than i thought!...by the way if your government agency is not good enough at data mining to FIND an individual's Facebook/twitter account when you have their name address and date of birth...then its time they just give up all pretense at offering any kind of security!. Besides which if someone wished to access the usa do you not think that just creating a dummy social media page and giving that info would be what they would do !...this is a waste of government money to monitor and our time and effort as travelers.

---

Comment Submitted by David Busch

**Comment**

View document:

I am simply appalled at this proposal.

Freedom of travel is one of the primary rights guaranteed in UN documents to which the United States subscribes--this proposal would grossly violate those covenants.

Unwarranted procedures to pry into people's affiliations or internal beliefs such as this, do nothing to

make America safer--they erode international respect for our core values, and do grave damage to U.S. interests. This proposal simply grossly violates and impinges on the principles of those internationally guaranteed rights--as well as our own principles of freedom and privacy within our own US Constitution.

Just this, their appalling consideration, will no doubt be now an international embarrassment--in the world's perception of the United States:

--as an upholder of freedoms and democracy.

As an American citizen, I am appalled and adamantly oppose this measure.

---

Comment Submitted by Damien Sullivan

**Comment**

View document:

I believe the proposal is creepy, intrusive, and unnecessary. Even if officially "optional", it will not come across that way in the power-imbalanced context of getting some unknown official to allow one into the country. I'd expect that any competent 'nefarious' people would refuse to answer or give dummy accounts, so this becomes mostly a big waste of time for travelers, coupled with a potential for abuse by customs officials looking up such accounts and harassing people based on what they find, or for having refused to answer. I'd fear that this would become a stepping stone to required disclosure, as well.

---

## Comments August 15-19, 2016

---

Comment Submitted by John Pearson

Comment

View document:

Although the United States may not actually be "The Home of the Free and the Land of the Brave" our government agencies should at least STRIVE toward that ideal. Alas, in wanting to enact this regulation CBP officials are Orwellian cowards who seek to violate people's implicit Constitutional right to privacy. Is this the message we want to send to foreigners, that the American people seek to violate your basic human rights? But moral and public relations concerns aside, the main reason to not enact this regulation is a practical one: The potential waste of agency resources. I fear that considerable manpower could be spent essentially looking for a needle in a haystack when CBP agents should be concentrating on reducing bridge wait times (I live in El Paso, Texas). For the sake of your agency, the American people and foreigners seeking entrance to this sometimes great land of ours, please do not waste your time and taxpayers' money poring over private social media accounts.

---

Comment Submitted by Michael Tanzer

Comment

View document:

This is so wrong, They can't do that! It's like they're stealing our freedom of speech! Censoring online speech is NOT right! We have the right to post anything we want! This is NOT North Korea or China!

---

Comment Submitted by Anonymous

Comment

View document:

please no

---

Comment Submitted by Botond Ballo

Comment

[View document:](#)

This is an all-around bad idea.

First, it would not be effective in identifying people with intentions to harm the United States. The small minority of people with such intentions are very unlikely to post their plans online using social media accounts and then provide those same accounts when crossing the border.

Second, it's an invasion of privacy. The vast majority of information shared using social media accounts is personal and government officials have no business looking at it.

Third, collection of this information would open up travellers to discrimination based on protected grounds such as their religious or political beliefs, insofar as these beliefs are expressed in their social media accounts. The threat of such discrimination will lead to self-censorship and a chilling effect on free speech.

-----  
Comment Submitted by John Smith

Comment

[View document:](#)

This puts an unfair burden on the applicant to disclose information that may be taken out of context or can be easily misconstrued. It is a poorly designed "optional" requirement that does not take into account the laws of the US, the laws of the nations from which the applicant is coming, nor the highly subjective nature of the information posted to these types of online sites.

-----  
Comment Submitted by Anonymous (Concerned Citizen)

Comment

[View document:](#)

Why make it 'Optional'? The "nefarious" persons you are looking to catch aren't likely to hand over their online identities, so either drop a bird-brained idea or go off the deep end and make this invasion of privacy a requirement to enter the country.

-----  
Comment Submitted by Corey Cohen

Comment

View document:

I absolutely oppose this change proposed by US Customs and Border Protection. Asking people to submit their online handles will do nothing to identify people who should not be entering the US and will only serve to invade people's privacy and allow government agencies to develop full profiles on people who have done no wrong, broken no law and are under no suspicion. Collecting such information is irrelevant as anyone who did wish ill would not post such things publicly and, even if they did, would not provide the credentials to US officials simply because asked.

Stating that it is only an optional field does is no argument either. Anyone who refused to fill out this "optional" field would instantly be placed under suspicion, as if they had something they wished to hide. There would be obvious pressure to fill out said "optional field" that would make it far less optional than you make it out to be.

This provision is far to open, far too broad, far to invasive and would do nothing to help identify any dangerous persons to begin with.

---

Comment Submitted by David Lee

Comment

View document:

As an American, I oppose the addition of this question to travelers entering the US. Reviewing a social media account, even if it is optional or publicly available information, is like following around someone to watch what they are doing throughout the day. This is overreaching too much into personal privacy and is starting from our American ideals. Surely it won't be easy, but we can do better than this.

---

Comment Submitted by Lori Kingery

Comment

View document:

Please, don't do this.

Collecting the "social media" information for everyone legally entering the U.S. is security theater a la Bruce Schneier\*\* at its worst, placing undue (and extremely ill-defined!) restrictions on every law-abiding guest of the United States, while doing almost nothing to identify or apprehend those that are willing to circumvent the law.

In addition to squandering the limited physical and financial resources of U.S. Customs

and Border Protection (which would definitely negatively impact our collective security, as well as--much less importantly--taxpayer dollars), this measure surrenders freedom and free speech for precious little gains in actual security. It is security theater, designed to make us "feel" safer without actually measurably improving our actual safety.

Again, please...don't do this.

\*\* [https://www.schneier.com/essays/archives/2010/05/worst-case\\_thinking.html](https://www.schneier.com/essays/archives/2010/05/worst-case_thinking.html),  
[https://www.schneier.com/essays/archives/2013/01/unsafe\\_security\\_a\\_so.html](https://www.schneier.com/essays/archives/2013/01/unsafe_security_a_so.html)

p.s. Respectfully, removing the white space and newlines from comments not only detracts from readability for the recipient, it changes the tenor, tone, and flow of the writer's message, negatively impacting both ends of the communication equation. Whomever governs this comment-gathering device, please consider passing our detailed and thoughtful communications through as written, rather than compressing them to save a tiny bit of space.

---

Comment Submitted by Michael Sholinbeck

Comment

View document:

If enacted, social media collection by CBP will invade individual privacy, burden free expression, and expose particular communities to the risk of undue surveillance or ideological exclusion. The price of a business trip or family vacation to the United States should not include a fishing expedition into one's beliefs, reading lists, tastes, and idiosyncrasies by Customs officials. This regulation does not seem to significantly improve security such that this level of privacy invasion is warranted. Thank you.

---

Comment Submitted by David English

Comment

View document:

Making those who enter the US provide their social media accounts is an invasion of privacy and would make people self-censor their speech. As an American I feel this is a very bad idea and a bad precedent in screening people. My wife is a foreigner and I can't imagine her having to give up that personal information in order to enter the US to visit my family.

---

Comment Submitted by Carlos Pujols

Comment

View document:

HOLA UNA PREGUNTA. ES POSIBLE QUE TENGA PROBLEMA CON UNA LETRA QUE ME FALTA A MI ULTIMO APELLIDO TERMINA EN ( LS ) Y SOLO TENGO PUESTO EN EL VISADO ( L ).

ESTO ME DARA PROBLEMA A LA HORA DE VIAJAR. GRACIAS

To Whom It May Concern:

I think it unwise to elect to include the optional question field for social media identifiers/username. These are largely public profiles to begin with and are readily available to be found without this information. To ask this information of someone, even optionally, may make them feel coerced into doing so for fear of further scrutiny. I for one am not for creating an air of fear in immigrants.

There are also just some things the government does not need their hands in. Usernames to social media profiles is one of them. No explanation of how, where or for how long this information is stored is proposed to be provided. It is not morally correct to ask this of people without full disclosure of how and for what this is to be used for.

Most importantly what will it accomplish? Anyone who would be trying to harm this country or the citizens of it will become aware of these with time and either create fake profiles or change their identifiers or not put anything at all! It just means more money spent for no reason.

In short the only thing to come of this is fear, profiling, and more unwarranted monitoring of people's personal lives. It is a terrible idea with the best of intentions and should not be implemented.

Thank you for your consideration.

Regards,



Charles Miskolc



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.

Dear Sir or Madam,

I write today about the proposal to change the i-94 and ESTA form to request social media accounts of people traveling to the United States.

I have worked in technology, making consumer products for the last 8 years. Before that, I worked on enterprise software, and taught technology to high school students.

I'm alarmed at the proposal by DHS to request social media accounts of people entering the country.

This is a bad idea. Even if it is optional today, it may become a requirement in the future - and so should not be asked today, optional or not.

The argument that governments need to keep tabs online to ensure that people entering the country refrain from inappropriate or illegal behavior doesn't really hold. While it's conceivable that some low level silliness, such as posting a picture of yourself dancing on a table, could be prevented by employer monitoring, more serious infractions are unlikely to be shared on social media.

In addition, when people know that they are being watched, they can restrict access to certain posts, set up dummy profiles to avoid monitoring, or otherwise throw up smokescreens. This is particularly true of millennials, who are technologically adept at controlling and manipulating their online avatars. The point is, the limited preventative effect of social media monitoring is not worth the time and expense required for CBP to do it.

There is also the problem of bias. People today are arguably more socially and politically conscious than previous generations and actively use social media to convey their thoughts, and debate important topics. In some cases, CBP officers may even be supportive, such as if a person traveling works tirelessly to raise money for breast cancer research, but in other cases, there is a real danger of people being penalized for their personal views on subjects like politics, race, or religion.

The proposal says:

"DHS proposes to add the following question to ESTA and to Form I-94W: "Please enter information associated with your online presence—Provider/Platform—Social media identifier." It will be an optional data field to request social media identifiers to be used for vetting purposes, as well as applicant contact information. 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."

In truth, it will do none of these things:

- It will NOT enhance the investigative process in any meaningful way.
- It will NOT provide DHS with greater clarity and visibility to nefarious activity or connections.

There's a saying, "Garbage In, Garbage Out." Adding more garbage won't result in greater clarity.

This proposal should be withdrawn.

Thank you.

188 Suffolk St., Apt. 3A  
New York, NY 10002  
m@mlcastle.net

June 25, 2016

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

Re: Docket Number USCBP-2007-0102, "Proposed Collection; Comment Request;  
Arrival and Departure Record: (Forms I-94 and I-94W)"

Dear Officer:


I write in regard to *Federal Register* docket number USCBP-2007-0102, your office's proposal to begin asking visitors to the United States for their social media identifiers. This proposal is severely flawed and should be abandoned.

By your own office's estimation, the cost to the public of this new regulation will be nearly \$300 million. The benefits to the public, however, are likely to be far smaller: as the question is to be optional, it is easy to see that very few terrorists will voluntarily provide social media profiles where they express support for terrorism, and therefore the law enforcement benefit from this question is likely to be extremely small.

Beyond this, the cost to the American economy of this modification of the form is likely to be still higher than your estimate. Some legitimate foreign travelers, upon learning of this new addition to the travel requirements, may abandon their travels to the United States out of a desire to preserve their privacy. This—likely high—cost to the tourism and related industries is not accounted for in your proposal.

Given the worrying privacy implications of the proposal, combined with its high cost and likely low effectiveness as a law enforcement tool, I urge you not to implement it.

Sincerely,



Michael Castleman



Robert Peterson  
5162 Holmes Pl  
Boulder, CO 80303

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

Dear U.S. Customs and Border Protection:

I oppose your proposal (81 FR 40892) to add questions to ESTA and Form I-94W concerning social media presence. The generalized collection of online identities or identifiers on social media platforms is not an appropriate activity of the government. By their nature, online identities offer the possibility of anonymity, which many citizens make use of to exercise free speech. Many rely on anonymity for reasons of personal security, making your proposal a troubling shift in the nature of electronic free speech that is inappropriate for Customs and Border Protection to pursue. The "voluntary" nature of this information request still implies that government collection of social media information is acceptable, which I do not believe.

Finally, requiring written comment on this proposal, rather than providing for electronic submission of public comment, places a burden on interested members of the public. Given the nature of the proposal, this excludes those citizens most affected, i.e. users of social media and other forms of digital communication. It is also an irony that public comment must be addressed, in writing, to the Paperwork Reduction Act Officer. I ask you to rescind your proposal, and allow for electronic submission of public comment for future proposals.

Sincerely,



Robert Peterson

**Title:** Arrival and Departure Record, Nonimmigrant Visa Waiver Arrival/Departure, and Electronic System for Travel Authorization (ESTA).  
**OMB Number:** 1651-0111  
**Form Numbers:** I-94 and I-94W.

**Question:** "Please enter information associated with your online presence—Provider/Platform—Social media identifier."

**(a) Whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility;**

No, the information is not "necessary for the proper performance of the function of the agency." This type of electronic threat modelling is already conducted by sister organizations (e.g. NSA, DHS) and rather than relying on self-incrimination, they actively monitor social media for threats, even those which aren't self-reported.

Additionally, a lot of social media accounts won't have any public information available. So you'll be collecting, storing, and checking on accounts which won't provide any useful intelligence or any intelligence at all in some cases. A 2013 Pew Research Center study found, "[Only] 14% of teens say that their profile is completely public."

That also assumes members of the public even provide you with social media accounts with actionable intelligence. Some may choose to provide unused accounts, old accounts, or accounts with less incriminating posts on it. Alternative they could actively remove posts after answering the question itself. So I'd strongly question what practical utility can be obtained. You really are asking people to incriminate themselves, and even then only in situations where their privacy controls allow you to view any information at all. Even with this question for the vast majority of travelers you'll see increase cost but no utility.

**(b) the accuracy of the agency's estimates of the burden of the collection of information;**

Where is the cost of actually acting on this information? You spent hundreds of millions of dollars collecting this information, but this information only gains theoretical utility when you go out and review these social media profiles (many of which will be private anyway), that too has an inherent cost. But the cost of using the information isn't included, only the cost of collecting it. So the figures provided massively under-report the true cost of this project.

Plus, once you collecting incriminating posts, how are those transmitted from the back end team to the front end agents? And how does the system flag different levels of social media



information? Does everyone with any intelligence from social media get stopped and interviewed? Is the initial agent meant to quickly review it and make a determination? What is the cost of developing back-end systems with this?

You've actually misunderstood the entire scope of the collection thus under-reported it. This information collection is both on the forms but also from social media sites themselves. So until you tell us the cost of collecting a single social media post from social media and delivering it to a front end agent, you haven't even begun to show the full cost to the public of this project.

At the current time, with the way the costs are written, you won't be using this social media information which means it should be rejected for being useless. If you do plan to use it then the cost as written are misleading, since they exclude too much.

**(c) ways to enhance the quality, utility, and clarity of the information to be collected;**

This question is predicated on the assumption that this information should be collected, an assumption I reject. This entire concept is just going to wind up with a bunch of junk information about fake accounts or accounts that no longer exist. The few that do exist won't be accessible thus also being pointless.

**(d) ways to minimize the burden including the use of automated collection techniques or the use of other forms of information technology; and**

You can minimize it by discontinuing it.

**(e) the annual cost burden to respondents or record keepers from the collection of information (total capital/startup costs and operations and maintenance costs).**

As I said above, the costs are massively under-reported. You need to also calculate the data collection cost of using this information. Without that estimate this entire project makes no sense, this information only gains utility when used, and for this information to be used you need to spend money. Where are the cost estimates?

Regards,  
James Godfrey

U.S. Annual and Expense Report System (U.S. Annual Report System)  
U.S. Annual Report System (U.S. Annual Report System)  
U.S. Annual Report System (U.S. Annual Report System)  
U.S. Annual Report System (U.S. Annual Report System)

U.S. Annual Report System (U.S. Annual Report System)  
U.S. Annual Report System (U.S. Annual Report System)  
U.S. Annual Report System (U.S. Annual Report System)  
U.S. Annual Report System (U.S. Annual Report System)

June 30, 2016

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

Re: [USCBP-2007-0102](#)

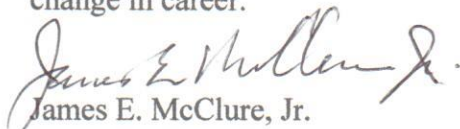
Dear Sirs:

With regard to the US Customs and Border Patrol's request that the question "Please enter information associated with your online presence – Provider/Platform – Social media identifier" be added to the Electronic System for Travel Authorization (ESTA) and to the CBP Form I-94W (Nonimmigrant Visa Waiver Arrival/Departure), I have many questions, but one immediately comes to mind as being particularly pertinent: Are you f\*\*\*ing kidding me?

Let me first state that I am aware the federal government – actually ANY government – is always infected with the idiocy virus, but it usually is of a low level, non-virulent strain. In this case, whoever thought of this idea has a really bad case of it and needs to be fired or, perhaps, promoted to the position of Director of the Office of Really Bad Ideas. The reasons this request is a bad idea:

1. There is the inconvenient fact that nothing would stop evil-doers from lying about their social media presences.
2. There lies the distinct possibility of people providing fake account names. Would innocent people suddenly find the feds at their door because CBP has "evidence" connecting their social media accounts with illegal acts?
3. There's always the possibility that a fake account can be created by someone impersonating the person the CBP is interested in.
4. Finally, the question, if the request passes, is optional—for now. However, as we all know, this is the perfect stepping stone for making answering that question mandatory in the future. Talk about a slippery slope.

Please show a modicum of intelligence and withdraw this request. It will save someone an involuntary change in career.

  
James E. McClure, Jr.  
12507 N. Hickory Grove Rd.  
Dunlap, IL 61525-9411

P.S. I'm NOT on social media



July 3, 2016

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

Subject: Comment on Federal Register Notice (Vol. 81, No. 121, Pages 40892-40893, June 23, 2016)  
regarding *Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and  
Electronic System for Travel Authorization*

Dear Paperwork Reduction Act Officer:

I welcome the opportunity to emphatically disagree with the proposed collection of the personal social media data of travelers arriving in (or returning to) the United States.

While I grant DHS the benefit of the doubt with regards to the sincerity of the intended purpose of this proposed change, sincerity does not prove the wisdom of an idea. My specific concerns are as follows:

How will DHS (or CBP) define "online presence" and "social media"? Is this limited to Facebook or LinkedIn or Twitter? But what about Amazon or eBay or iTunes where comments or reviews are posted? What about blogs? What about comments submitted on the websites of newspapers or other media entities? What about personal e-mail and texting accounts? Or online banking? Or hotel, airline, ride, or rental car web accounts? All of these web platforms can be considered to be "online presence" or "social media."

Speaking personally, I have a number of accounts that I use with varying frequency. But frankly, I, like surely many other people, cannot remember all of the screen names I use. Many of them I never need to remember because my home computer auto-fills that field. Therefore, it is unrealistic to expect the average traveler to be able to accurately list this information from memory upon entry into the country.

The proposed notice states this data will "provide DHS greater clarity and visibility to possible nefarious activity." If I were a traveler who intended to engage in nefarious activity, why would I provide this information if it could be used by DHS to thwart my intentions? So while enhancing DHS' investigative efforts is an admirable idea, the proposal to collect this data would probably provide little if any practical benefit.

But regardless of any objections I have about the practicality and effectiveness of this proposed data collection, my main objection is ideological. The proposed notice claims this data will be collected in an "optional" data field, but this is a slippery slope. Will the form clearly tell the traveler that providing this data is not mandatory? What if a traveler decides to leave this field blank? How will this be perceived by CBP? Will it raise suspicions and prolong the entry process? What if he provides information that is incorrect because he honestly misremembered it? So again, why would anyone—whether or not they have nefarious intentions—want to provide this data, especially if doing so is optional?

The mass collection by government of personal data is never a good idea unless it serves an unambiguously necessary purpose, effectively implemented. Here, we have a bureaucratic data collection idea that will be a waste of time and taxpayers' money.

Sincerely,



Michael Smithson



June 5<sup>th</sup>, 2016

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.

I am writing in response to the notice published in Federal Register on 6/23/2016 entitled "Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization"

I am responding to the question of "whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility."

The proposed changes to the I-94W and I-94 forms, albeit small, have potentially grave ramifications to the fundamental ideals upon which the United States is founded and practically will result in no net improvement to the security of the country.

#### **Constitutional Problems – Chilling effect on speech**

In 1996, a three judge panel from the Eastern District of Pennsylvania declared the Communications Decency Act unconstitutional. Judge Dalzell, writing the opinion of court, declared: "[T]he Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the **Internet deserves the highest protection from governmental intrusion** (emphasis added)."

The Internet, in its present form, is used by billions of individuals around the world to communicate with each other. Whether it is for business, pleasure, entertainment, enlightenment or political discourse, social media on the Internet is perhaps the principle forum today by which people of diverse cultures, countries and mindsets interact on a daily basis. Ostentatiously, the objective of the form change, is to identify social media profiles of visitors to the United States. The social media profiles will be reviewed and analyzed, whether by automated or manual means. Potentially, individuals whose social media profiles indicate they are in some way threatening to the United States, will be prohibited from entry, or their entry will be more closely scrutinized.

What is more likely the outcome is that

- (1) Individuals with controversial writings will choose not to visit the United States, reducing the diversity of ideas and discussion on those topics (within the geographic United States).
- (2) Individuals with controversial thoughts will scrutinize their social media presence and avoid discussions on those thoughts on what Judge Dalzell called "a never-ending worldwide conversation." This will reduce the diversity of ideas and discussions on those topics (on the Internet).

The chilling effect is not just on foreign nationals but negatively affects the ability of United States citizens to listen to and discuss controversial topics with foreigners abroad. In 1965, the Supreme Court in *Lamont v. Postmaster General*, 381. U.S. 301 struck down section 305 of the Postal Service and Federal Employees Salary Act because it required the Postmaster General to detain foreign mailings of communist political propaganda unless the addressee affirmatively acknowledge their acceptance and desire to receive such material. The Supreme Court recognized that this would reduce the recipient's unfettered access to constitutionally protected speech, and thus the act was unconstitutional. The courts have consistently ruled that acts of government, even when they do not have a direct prohibition on speech, but have a chilling effect, are never the less, unconstitutional. This change to form I-94 and I-94W will have a similar effect.

As to the necessity of the proposed change to the function of the agency, an unconstitutional act can never be necessary.

### **Practical Utility of the proposed change**

Selection bias is defined as "selection of individuals, groups or data for analysis in such a way that proper randomization is not achieved, thereby ensuring that the sample obtained is not representative of the population intended to be analyzed." The simple fact is that those attempting to enter the United States to perform terrorist acts are simply not going to list their Jihadi forum screennames on the I-94 forms. Those filling out this optional section are most likely to be people who believe the mundanity of their social presences leaves them immune from any issue with entering the U.S. This will result in three practical problems:

- (1) While Facebook, Twitter and a few others constitute the biggest players in social media, there are thousands upon thousands of smaller social media sites catering to every niche, minority and social group. Further, many people maintain multiple identities on different platforms. Any collection of information will, no doubt, be incomplete.
- (2) Large amounts of data from visitors who pose no threat will be collected, resulting in wasted effort and resources by the government to review that data, whether by automated or manual means.
- (3) Since many of the most threatening visitors or potential visitors will provide no or sanitized information only, the most likely people that this is going to stop are those whose social media posts or connections are taken out of context or who, while not representing a threat to the U.S., have controversial views. This will result in investigatory efforts into and dealing with appeals from individuals who have wrongly denied entry. Additionally, for those that are denied entry, it will result a chilling effect and inability for those in the U.S. to interact, learn from and discuss topics with the denied party.

The net result is the proposed change is likely subject to a claim of unconstitutionality and practically will not achieved the desired ends.

Sincerely,



R. Jason Cronk, Esq.  
Florida Bar #90009



## **Comments of the Center for Democracy & Technology**

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

19 August 2016

The Center for Democracy & Technology appreciates the opportunity to provide comments to the Department of Homeland Security on its proposal to begin requesting disclosure of social media identifiers and other online account information from Visa Waiver Program applicants. DHS proposes to ask foreign visitors applying for a waiver of visa requirements to provide “information associated with [their] online presence,” including the “provider/platform” and “social media identifier” used by the applicant. While the details of this proposed information collection are unclear, DHS’s Notice of Collection Activities states that the solicited online identity information “will enhance the existing investigative process” and “provide DHS greater clarity and visibility to possible nefarious activity and connections” of visitors to the United States.<sup>1</sup>

CDT is deeply concerned that this proposal would invade the privacy and chill the freedom of expression of visitors to the United States and United States citizens.

Under the proposed changes, visitors to the U.S. who seek admittance through the Electronic System of Travel Authorization (ESTA), or complete Form I-94W, will be subject to unspecified review and monitoring of their public online activity by U.S. Customs and Border Protection (CBP) officials. This program will also increase the surveillance of U.S. citizens, both as a result of their online connections to visitors to the U.S. and because other countries may seek similar information from U.S. citizens traveling abroad. The burdens of this scrutiny will undoubtedly fall disproportionately on visitors and U.S. citizens who are Muslim or who have connections to the Middle East.

In addition to these challenges for fundamental rights, the proposal has a number of practical drawbacks as well. First, it is unlikely to yield useful information for CBP officials. Bad actors could easily circumvent the request by providing intentionally false or incomplete information. Further, the expense of the proposed data collection and analysis is significantly underestimated in the Request for Comment. In-depth, unbiased evaluation of a prospective visitor’s public social media posts and connections cannot be accomplished in an automated fashion and would require extensive—and costly—human review.

For all of these reasons, we urge DHS to withdraw this proposal and to reject any approach that involves suspicionless monitoring and review of individuals’ social media activity.

---

<sup>1</sup> U.S. Customs & Border Protection, Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization, FederalRegister.gov (June 23, 2016), <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> (hereinafter “Federal Register Notice”).

## **I. Requesting disclosure of online identifiers in the Customs process would create a significant burden on the free expression and privacy of international travelers.**

The proposed information collection would affect visitors who are traveling with a passport issued by one of the Visa Waiver Program designated countries, including Japan, South Korea, Singapore, Chile, Taiwan, and many members of the European Union and other European countries.<sup>2</sup> If arriving by air or sea, these travelers must fill out an ESTA form at least 3 days before their intended arrival to the U.S. and renew it at least every two years. In 2014, over 22 million visitors entered the U.S. through the Visa Waiver Program.<sup>3</sup> In addition to tourists, this includes family members, patients, amateur athletes and musicians, scholars, conference attendees, business visitors, and entrepreneurs.<sup>4</sup>

The scope of these visitors' online activity is enormous, and the proposal provides no definition of "online presence", "provider/platform", or "social media identifier" to narrow the field. This creates the potential for an overly broad or arbitrary interpretation by CBP officials or applicants who are concerned about being denied a visa waiver. Millions of websites and online services allow, and sometimes require, users to create a username or other identifier to post content and connect with other users. In the realm of travel-related services alone there are dozens of sites and apps that might fit the bill, including TripAdvisor, Yelp, AirBnB, VRBO, Couchsurfing, Hostelworld, Uber, Lyft, Tripatini, Google+ (including Google Maps and Translate), Foursquare, and WikiTravel. Or DHS may be focused on more general-purpose services such as Facebook, Twitter, YouTube, SnapChat, Instagram, Pinterest, Tumblr, Reddit, LiveJournal, XING, StudiVZ, Hyves, Fotolog, KakaoTalk, LINE, WeChat, Pixnet, Xuite, Plurk, or even dating services such as Tinder, Grindr, and OKCupid. Any of these, and thousands more, could represent a portion of an individual's "online presence". DHS has provided no explanation of what type of response it expects from visitors.

While the Request for Comments describes the request for applicants' social media identifiers as "an optional data field," applicants for a visa-waiver will likely feel compelled to disclose significant amounts of personal information in response to this question. The majority of the data fields on the ESTA form are mandatory, and absent a specific indication to the contrary, it is likely that applicants will presume this question is mandatory as well.

---

<sup>2</sup> A full list of Visa Waiver Program designated countries is available at 8 C.F.R. § 217.2.

<sup>3</sup> 2014 Yearbook of Immigration Statistics, *available at* [https://www.dhs.gov/sites/default/files/publications/table28d\\_7.xls](https://www.dhs.gov/sites/default/files/publications/table28d_7.xls). In 2010, Visa Waiver Program visitors contributed over \$60 billion in tourism revenue. The White House, Office of the Press Secretary, Obama Administration Continues Efforts to Increase Travel and Tourism in the United States (May 10, 2012), *available at* <https://www.whitehouse.gov/the-press-office/2012/05/10/obama-administration-continues-efforts-increase-travel-and-tourism-unite>. The U.S. Travel Association estimates that, in 2015, Visa Waiver Program visitors "generated \$120 billion in total output for the U.S. economy, supporting nearly 800,000 American jobs." U.S. Travel Association, Visa Waiver Program, *available at* <https://www.ustravel.org/issues/visa-waiver-program>.

<sup>4</sup> U.S. Department of State, Bureau of Consular Affairs, Visa Waiver Program, *available at* <https://travel.state.gov/content/visas/en/visit/visa-waiver-program.html>.

Even if this question is clearly marked “optional”, however, most applicants will likely feel substantial pressure to provide some information in response, because it is unclear whether refusing to provide this information could result in CBP officials drawing adverse inferences. The consequences of a visa-waiver denial to the visitor, her family, her business associates, and her fellow travelers can be significant. Travelers are able to fill out an ESTA application online at their convenience. The form takes an average of 20 minutes and there is a \$14 fee per application.<sup>5</sup> In contrast, visa applications require the applicant to visit a consulate in person and can take months to process.<sup>6</sup> Assuming the traveler has enough time to apply for a visa after being denied a waiver, the B1 visa costs at least \$160, plus any expenses incurred traveling to a consulate to apply in person.<sup>7</sup> As a result, if a traveler’s ESTA application is rejected, that traveler could be prevented from coming to the U.S. entirely. This creates a considerable incentive to respond thoroughly to every question asked in the waiver-request process.

Potential visitors to the U.S. will thus be faced with a choice between two undesirable options: decline to disclose information about their online identity and risk being denied a waiver for providing incomplete information, or disclose this information and risk denial due to inaccurate or prejudicial inferences made about their online activity. It is unclear what sort of online activity CBP officials would consider to merit denial of a visa waiver; as we discuss below, evaluation of public social media posts and connections for accurate, actionable intelligence is an extremely complex task. As a practical matter, applicants would have little or no opportunity to explain information associated with their online profiles or challenge inappropriate denial of a visa waiver. And, while denial of a person’s visa-waiver request does not preclude their entry to the U.S. by a standard visa, most travelers would reasonably assume that an adverse decision on their ESTA application would translate to a similarly adverse decision on the issuance of a visa.

Thus, this proposal will create a chilling effect for travelers wishing to come to the U.S.<sup>8</sup> The risk of denial based on their online presence could lead some visa-waiver applicants to delete sensitive or controversial accounts in preparation for travel to the U.S., or simply to forgo an online presence at all. The strong incentives to disclose, and the unknown risks of nondisclosure, will compel many other applicants to share abundant information about their online activity. Most of these innocent disclosures will be useless for screening purposes, but they may still be used to augment the growing intelligence surveillance apparatus—with little legal protection for personal information and few, if any, mechanisms to safeguard against abuse.

---

<sup>5</sup> Department of Homeland Security, Official ESTA Application, <https://esta.cbp.dhs.gov/esta/>.

<sup>6</sup> Visas can take months to process. U.S. Customs & Border Protection, Frequently Asked Questions about the Visa Waiver Program (VWP) and the Electronic System for Travel Authorization (ESTA), <https://www.cbp.gov/travel/international-visitors/frequently-asked-questions-about-visa-waiver-program-vwp-and-electronic-system-travel>.

<sup>7</sup> U.S. Bureau of Consular Affairs, Visitor Visa, <https://travel.state.gov/content/visas/en/visit/visitor.html#fees>.

<sup>8</sup> See, e.g., Caution on Twitter urged as tourists barred from US, BBC.com (Mar. 8, 2012), <http://www.bbc.com/news/technology-16810312>.

## **II. The proposed collection is highly invasive and offers no assurances against abuse.**

Currently, the visa-waiver application solicits information about a prospective visitor's name, address, and citizenship, as well as topics such as their criminal background, health status, and whether they have overstayed a visa on a previous trip. While this information is certainly personal, the material associated with an individual's online presence can reveal a much deeper insight into a person's personality, preferences, ideas, and values. And the nature of social media technology in particular also exposes information about other people in their networks.

International travelers rely on social media and apps to find and purchase flights and accommodations, to find information about Customs procedures, to read and write travel reviews, to follow local news and make new connections, to communicate over long distances with colleagues, friends, and family back home, to contact their embassies or consular services in an emergency, and more. The DHS proposal would, in effect, ask travelers to give CBP a window into all of these online activities without clear standards for protecting those who disclose their online profiles and those in their networks.

Moreover, travelers may not be fully aware of the entire scope of information that they are disclosing. Many internet users have multiple social media accounts, sometimes dating back a decade or more. Visitors may list these outdated accounts, forgetting they contain posts and connections that are out of date. And even if a person withholds particular identifiers that are associated with sensitive content (e.g., a Grindr profile) or connections (e.g., a controversial Facebook group), investigators may be able to unearth these accounts based on the information that is disclosed.

Further, accounts on some social media sites routinely display third-party posts and comments that were added to the account owner's page without her knowledge or consent. Depending on the user's privacy settings, some of these posts could be from complete strangers. Such posts may contain inaccurate or deliberately misleading information. Social media login credentials can also be compromised, and accounts hijacked, to disseminate content that the person did not or would not post.<sup>9</sup>

A person's social media activity also necessarily reveals information about people in her social networks, including her family members, friends, and "followers"; therefore, disclosing a social media identifier to DHS could subject a person's close and distant associates to invasive scrutiny and exposure without their consent. This could create particular risks for journalists, lawyers, clergy, human rights workers, and others whose professions require confidentiality or who may face serious consequences if their social media profile were taken out of context. The recent experiences of a Wall Street Journal reporter pressured to give CBP access to her mobile devices<sup>10</sup> and an Al Jazeera journalist discovering

---

<sup>9</sup> See, e.g., Kate Conger, How activist DeRay Mckesson's Twitter account was hacked, Tech Crunch (June 10, 2016), <https://techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-account-was-hacked/>.

<sup>10</sup> Joseph Cox, WSJ Reporter: Homeland Security Tried to Take My Phones at the Border, Vice Motherboard (July 21, 2016), [http://motherboard.vice.com/en\\_uk/read/wsj-reporter-homeland-security-tried-to-take-my-phones-at-the-border](http://motherboard.vice.com/en_uk/read/wsj-reporter-homeland-security-tried-to-take-my-phones-at-the-border).

he was placed on an NSA watch list<sup>11</sup> highlight the risks such surveillance programs pose to civil society institutions including the free press.

Social media posts are also vulnerable to interpretive error. The content and conversation on a person's page or feed is highly context-dependent, making it prone to misinterpretation—particularly when the interpreter does not speak the language or lacks cultural, colloquial, or idiosyncratic touchstones necessary for accurate understanding of the content. Similarly, metadata, including contacts within a person's list of "followers" or "follows," can be easily misconstrued when divorced from the context of the connection. Without the contextual understanding that a person is a journalist or human rights researcher, for instance, her connection to violent extremist accounts could appear suspect.<sup>12</sup> People collect many diverse social media connections, and may not even be aware of the identity behind an account that they follow. In fact, one study found that the *majority* of friendships on Facebook are not based on a "real", non-casual relationship.<sup>13</sup> These features undermine the value of this data and increase the risk of erroneous denial of a visitor's ESTA application.

Finally, the proposal does not protect applicants from the risk of improper conclusions based on declining to disclose "online presence" indicators. If DHS discovers the existence of an undeclared account, will the applicant be flagged for additional scrutiny? Will CBP officials draw negative inferences from the privacy settings an applicant has placed on his accounts? These questions remain unanswered. The proposal describes no recourse for individuals who believe they were improperly denied a visa waiver, or subsequent visa application, based on their online presence.

### **III. Collecting online identifiers from visitors to the U.S. would be a significant expansion of U.S. intelligence activity.**

This proposal seeks to implement an intelligence-gathering program in the form of a Customs administration mechanism, under the auspices of the Paperwork Reduction Act. Data collected through the I-94W and ESTA forms is not limited to determining an applicant's eligibility for a visa waiver. DHS engages in massive collection and analysis of open-source data<sup>14</sup> and has invested in

---

<sup>11</sup> Cora Currier, Glenn Greenwald, & Andrew Fishman, U.S. Government Designated Prominent Al Jazeera Journalist as "Member of al Qaeda," *Intercept* (May 8, 2015), <https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/>.

<sup>12</sup> Human Rights Watch, *With Liberty to Monitor All: How Large-Scale U.S. Surveillance is Harming Journalism, Law and American Democracy*, July 2014, *available at* <https://www.aclu.org/report/liberty-monitor-all-how-large-scale-us-surveillance-harming-journalism-law-and-american>.

<sup>13</sup> R.I. Dunbar, *Do online social media cut through the constraints that limit that limit the size of offline social networks?*, *Royal Society: Open Science*, January 2016, *available at* <http://rsos.royalsocietypublishing.org/content/3/1/150292>.

<sup>14</sup> See Office of Inspector General, Dep't of Homeland Security, *DHS Uses Social Media To Enhance Information Sharing and Mission Operations, But Additional Oversight and Guidance Are Needed*, No. OIG-13-115 (September 2013), *available at* [https://www.oig.dhs.gov/assets/Mgmt/2013/OIG\\_13-115\\_Sep13.pdf](https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-115_Sep13.pdf).

systems of automated social media analysis.<sup>15</sup> Increased collection and retention increases the risk of data breach, as well as the potential for misuse and abuse. Harassment and fraud are among the biggest risks to users and institutions, such as banks or hospitals, when social media identifiers are breached.<sup>16</sup>

Further, all of the information collected through the visa-waiver program is shared, in bulk, with U.S. intelligence agencies and will be used to seed more intelligence surveillance unrelated to the applicant's eligibility for a visa waiver.<sup>17</sup> If this proposal is adopted, social media identifiers – tied to the true identity of visa-waiver applicants – will be shared with the National Security Agency which can then use the information to target applicants for surveillance. Data collected under this proposal would feed into intelligence surveillance for much broader purposes and without meaningful controls. Once in the Intelligence Community (IC), elements of the IC can then use the information provided to pursue their missions. This data is likely to be used to augment existing lists and databases for tracking persons of interest to law enforcement and intelligence agencies, with consequences for innocent individuals swept up in those surveillance programs. And to the extent the applicant's social media account reveals those with whom the applicant communicates (see discussion above), those persons can be targeted as well.

Under current law, Visa Waiver Program travelers – by definition, non-U.S. persons outside the United States – who are affected by expanded surveillance under this proposal will have no recourse against abuse. Specifically, surveillance under Executive Order 12333 is conducted without any judicial oversight. It can be conducted to collect “foreign intelligence information,” which includes information about the “activities” of any non-American abroad. Collection of information about these broadly defined “activities” is permissible even if there is no reason to believe that those activities threaten U.S. national security, are relevant to U.S. foreign policy, or are conducted by a person who is an agent of foreign power. Likewise, surveillance under Section 702 of the Foreign Intelligence Surveillance Act proceeds without meaningful judicial authorization, for broadly defined purposes, and regardless of whether there is information indicating that the target of surveillance is a criminal, a threat, or an agent of a foreign power. As non-U.S. persons, prospective travelers have only limited Privacy Act

---

<sup>15</sup> Ellen Nakashima, DHS monitoring of social media worries civil liberties advocate, Wash. Post (Jan. 13. 2013), [https://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gI1QANPO7wP\\_story.html](https://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gI1QANPO7wP_story.html).

<sup>16</sup> Tracy Kitten, Social Media Plays Key Role in Bank Fraud, Data Breach Today (Aug. 3, 2016), <http://www.databreachtoday.com/interviews/social-media-plays-key-role-in-bank-fraud-i-3277>.

<sup>17</sup> See, e.g., Department of Homeland Security, Privacy Impact Assessment Update Electronic System for Travel Authorization (ESTA), DHS/CBP/PIA-007(f), June 20, 2016, at 5, available at [https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-june2016\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-june2016_0.pdf) (“CBP will continue to share ESTA information in bulk with other federal Intelligence Community partners (e.g., the National Counterterrorism Center), and CBP may share ESTA on a case-by-case basis to appropriate state, local, tribal, territorial, or international government agencies.”).



protections under the Judicial Redress Act, and these do not provide a guarantee against intelligence surveillance that targets an individual's expressive activity.

The community impacts of this proposal will go far beyond the denial of an individual traveler's visa-waiver application. Data collection and data sharing within the government imposes serious privacy costs that fall disproportionately on certain groups.<sup>18</sup> Social networks, in particular, lend themselves to association fallacies that can impact entire communities. Persons who are, or are presumed to be, of Muslim faith or Arab descent already face a disproportionate risk of religious and ethnic profiling while traveling, including enhanced TSA screening measures, wrongful inclusion on national security watchlists, and discriminatory citizen complaints.<sup>19</sup> Including travelers' usernames, posts, and social media affiliations in the screening process will increase the dangers of "flying while Muslim," particularly where cultural and linguistic barriers create an elevated risk of misunderstanding. A traveler who is wrongfully denied a visa waiver because of a distinct Arabic name or theological posts will suffer unfair and unjustified travel delays. And, in the process, her social media friends and followers will also be swept up in social media profiling. To the extent that the traveler's social network overlaps with her religious and ethnic community, those individuals will also be exposed to increased scrutiny and its consequences for safety and privacy.

#### **IV. Americans will be swept up in social media collection and surveillance activities at home, and will face reciprocal disclosures requirements abroad.**

If this proposal is adopted, it will disproportionately affect Arab-Americans and Muslim Americans whose family members, guests, colleagues, and business associates are flagged or denied a visa waiver as a result of their online presence. Moreover, DHS – and, by extension, the rest of the Intelligence Community – will necessarily acquire information about Americans whose accounts are affiliated with those scrutinized and flagged profiles.

This proposal would create significant risks of ideological profiling, if travelers are subjected to elevated scrutiny merely because they have expressed a strongly-held religious or political belief

---

<sup>18</sup> See, e.g., Alvaro M. Bedoya, The Color of Surveillance, Slate (Jan. 18, 2016), [http://www.slate.com/articles/technology/future\\_tense/2016/01/what\\_the\\_fbi\\_s\\_surveillance\\_of\\_martin\\_luther\\_king\\_says\\_about\\_modern\\_spying.html](http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html).

<sup>19</sup> American travelers have been plagued by profiling based on skin color, language, attire, and other markers of religious and ethnic background. See, e.g., Catherine Rampell, Ivy League economist ethnically profiled, interrogated for doing math on American Airlines flight, Wash. Post (May 7, 2016), [https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doing-math-on-american-airlines-flight/?tid=a\\_inl&utm\\_term=.00e58cfbfc37](https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doing-math-on-american-airlines-flight/?tid=a_inl&utm_term=.00e58cfbfc37); Peter Holley, Muslim couple says they were kicked off Delta flight for using phone, saying 'Allah,' Wash. Post (Aug. 7, 2016), [https://www.washingtonpost.com/news/morning-mix/wp/2016/08/07/muslim-couple-says-they-were-kicked-off-delta-flight-for-using-phone-saying-allah/?tid=a\\_inl](https://www.washingtonpost.com/news/morning-mix/wp/2016/08/07/muslim-couple-says-they-were-kicked-off-delta-flight-for-using-phone-saying-allah/?tid=a_inl); Carma Hassan & Catherine E. Shoichet, Arabic-speaking student kicked off Southwest flight, CNN.com (Apr. 8, 2016), <http://www.cnn.com/2016/04/17/us/southwest-muslim-passenger-removed/>.

online. Ideological exclusion of visitors would deny Americans access to information and opportunities for cultural and educational exchange that spur creativity and innovation. And American businesses would suffer economic impacts when foreign scholars, colleagues, and investors are delayed or denied entry. Potential visitors may decide instead to censor themselves online, rather than risk exclusion, which would further diminish Americans' access to information and opportunity for informed debate. As a network, the value of the global internet is related to the size and engagement of its participants; withdrawal of certain groups or communities diminishes the value of a network for all members.<sup>20</sup>

Finally, if this proposal is enacted, Americans will likely face reciprocal social media disclosure requirements when traveling abroad. Customs and immigration policy is notoriously susceptible to reciprocity effects, and the U.S. Visa Waiver Program is no exception. Currently, for example, the European Commission is considering restricting visa-free travel for Americans and Canadians in response to the absence of a visa-waiver path for nationals of some EU member states.<sup>21</sup> Americans traveling to Iran, Iraq, Syria, or Sudan could face higher hurdles, including social media disclosure requirements, in retaliation for the U.S. decision to exclude any recent travelers or dual nationals of those countries from eligibility for a visa waiver.<sup>22</sup> And all countries could be incentivized to implement online identity disclosures in the event that the U.S. expands its social media inquiry to visa applications.

For Americans traveling abroad, reciprocal social media disclosure requests could create travel delays and legal risk for speech that is protected under the United States Constitution. In non-visa waiver countries with fewer legal safeguards, disclosure requirements could expose American travelers to serious consequences such as border interrogations, administrative detentions, and other more serious penalties for social media activity that offends customs or norms against homosexuality, female immodesty, or religious or ideological dissent.<sup>23</sup> Other states' use of social media screening as an element of border security has demonstrated the significant risk of ideological and ethnic profiling that these programs create.<sup>24</sup> For example, in 2014, the U.S. Consulate in Jerusalem noted that "U.S. citizen visitors have been subjected to prolonged questioning and thorough searches by Israeli

---

<sup>20</sup> See Yochai Benckler, *Wealth of Networks: How Social Production Transforms Markets and Freedom* (2007).

<sup>21</sup> Tara Palmeri & Maïa de la Baume, EU considers restricting visa-free travel for Americans, Canadians, Politico (Apr. 7, 2016), <http://www.politico.eu/article/eu-considers-restricting-visa-free-travel-for-americans-canadians/>. The U.S. sets visa policy on a country-by-country basis; some EU members are not part of the U.S. Visa Waiver Program. This has led the European Commission to re-examine its visa policies for the United States. *Id.*

<sup>22</sup> Paul Dallison, U.S. visa changes hit Europeans, Politico (Jan. 22, 2016), <http://www.politico.eu/article/us-visa-changes-hit-europeans-dual-nationality-iran-iraq-syria/>.

<sup>23</sup> See, e.g., the case of British national Stephen Comiskey, who was reportedly entrapped by Saudi police, jailed, and sentenced to death for homosexuality before the United Kingdom managed to negotiate his release. Nick Parker, Execution fear of gay Brit battered in Saudi, theSun.co.uk (Mar. 31, 2011), <https://www.thesun.co.uk/archives/news/463707/execution-fear-of-gay-brit-battered-in-saudi/>. Singapore, which also criminalizes same-sex sexual relations, is a visa-waiver country.

<sup>24</sup> Diaa Hadid & Joseph Federman, Israel asks Arab visitors to open emails to search, NBCNews.com (June 5, 2012), [http://www.nbcnews.com/id/47690140/ns/world\\_news-mideast\\_n\\_africa/t/israel-asks-arab-visitors-open-emails-search/](http://www.nbcnews.com/id/47690140/ns/world_news-mideast_n_africa/t/israel-asks-arab-visitors-open-emails-search/).

authorities upon entry or departure. Those whom Israeli authorities suspect of being of Arab, Middle Eastern, or Muslim origin [...] may face additional, often time-consuming, and probing questioning by immigration and border authorities, or may even be denied entry into Israel or the West Bank."<sup>25</sup> All Americans have an interest in ensuring that social media border-screening programs do not become an international norm.

## **V. Online identifier collection would be ineffective and will impose significant unaccounted costs.**

DHS indicates that collection of visa-waiver applicants' online identity information will "enhance the existing investigative process" for screening visa-waiver applicants.<sup>26</sup> DHS has previously argued that generally increasing ESTA data-collection will streamline the visa-waiver application process by reducing the number of false-positive matches between applications and terrorism watchlists.<sup>27</sup> These empirical arguments rest on several flawed assumptions.

First, the ease of circumvention undermines this program's utility. Individuals who pose a threat to the United States are highly unlikely to volunteer online identifiers tied to information that would raise any question about their admissibility to the United States. Such questioning is far more likely to yield a flood of profiles from unsuspecting travelers who feel compelled to disclose information. It may also prompt some travelers to create false or "dummy" accounts to shield their privacy—or to deliberately undermine CBP agents' investigations.

Second, sorting through the quantity of information included in an individual's online presence creates a tremendous and costly administrative burden. Information traditionally collected as part of the visa process (names, birthdates, and place of birth, for example) includes single data points that can be easily cross-referenced against prepared indices such as watchlists or hotspots for terrorism or infectious diseases. By contrast, social media identifiers will yield messy and multidimensional data sets. As discussed above, social media in particular is vulnerable to misinformation and misinterpretation errors. Further, one identifier can expand the available data by many orders of magnitude with no comparable qualitative increase in information or intelligence. Given that the average internet user has five social media profiles,<sup>28</sup> this proposal would introduce significant noise and little if any discernable signal to the visa-waiver screening process.

---

<sup>25</sup> U.S. Consulate in Jerusalem, Entering and Exiting Jerusalem, the West Bank, and Gaza, <https://jru.usconsulate.gov/u-s-citizen-services/local-resources-of-u-s-citizens/entering-exiting/>; see also Adam Taylor, These accounts from Arab Americans show why an Israeli visa waiver plan is so controversial, Wash. Post (Apr. 27, 2014), <https://www.washingtonpost.com/news/worldviews/wp/2014/04/27/these-accounts-from-arab-americans-show-why-an-israeli-visa-waiver-plan-is-so-controversial/>.

<sup>26</sup> Federal Register Notice, *supra* n.1.

<sup>27</sup> U.S. Customs & Border Protection, Strengthening Security of the VWP through Enhancements to ESTA, <https://www.cbp.gov/travel/international-visitors/esta/enhancements-to-esta-faqs>.

<sup>28</sup> Jason Mander, Internet users have average of 5.54 social media accounts, GlobalWebIndex.net (Jan 23, 2015), <http://www.globalwebindex.net/blog/internet-users-have-average-of-5-social-media-accounts>. The average

Third, transforming raw social media data into actionable intelligence will require new capabilities in machine learning and complex network analytics—increasing costs and introducing new sources of error into the screening process. There may be useful data points that could produce insights or investigative leads amid the deluge of irrelevant and potentially false information gathered in response to this question. But, given the complexity of the dataset, CBP officers cannot conduct a cursory analysis. Even in combination with simple algorithmic screening against prepared databases and indices, this type of analysis is minimally accurate. Currently, machine learning used to identify jihadist accounts on Twitter exhibits an error rate of 10 to 24 percent.<sup>29</sup> Such an error rate would represent between 2 and 5 million annual visitors being falsely flagged under the Visa Waiver Program.<sup>30</sup> And because these algorithms are biased against foreign languages, particularly those not based on the Roman alphabet, the error rate for algorithmic assessment of social media information collected under this proposal will likely be even higher. By using unreliable and misleading social media activity as a proxy for admissibility, DHS will experience an increase in incidence of false-positive error.<sup>31</sup>

Moreover, machine learning can also introduce false negatives into a risk assessment. For example, if an algorithm is trained to identify whether an applicant is a person of interest, a positive match between an applicant's name and biographical information and an identity on a terrorism watchlist will result in a red flag. However, when social media information is added to the evaluation, there is a risk that it can contradict or discredit a database match, removing a correctly identified red flag from the application.<sup>32</sup> Given that machine learning processes introduce serious risks of both false-positive and false-negative signals, the necessity of human review cannot be avoided.

The more deeply a CBP investigator delves into an applicant's social media profile, however, the more training and context she will need in order to overcome the interpretive errors inherent in social media content and connection analysis. Some of the best technology in use today for identifying ISIS accounts

---

social media user posts frequently and has the ability to post various types of data. A majority of Facebook, Instagram, and Twitter users post at least once per week. Maeve Duggan et. al, Frequency of Social Media Use, Pew Research Center (Jan 9, 2015), <http://www.pewinternet.org/2015/01/09/frequency-of-social-media-use-2/>.

<sup>29</sup> Enghin Omer, Thesis: Using machine learning to identify jihadist messages on Twitter, Uppsala University, Sweden, July 2015, <http://uu.diva-portal.org/smash/get/diva2:846343/FULLTEXT01.pdf>.

<sup>30</sup> 2014 Yearbook of Immigration Statistics, *available at* [https://www.dhs.gov/sites/default/files/publications/table28d\\_7.xls](https://www.dhs.gov/sites/default/files/publications/table28d_7.xls).

<sup>31</sup> Sarah Foxen & Sarah Bunn, Forensic Language Analysis, 509 POSTnote (Sept. 2015), <http://www.forensiclinguistics.net/POST-PN-0509.pdf>.

<sup>32</sup> This effect is a byproduct of algorithmic decisionmaking: Risk-assessment algorithms rely on various qualifying criteria to determine whether an entry can be identified as "suspicious." If the various fields of data pertaining to an entry reinforce each other, this can increase the algorithm's accuracy. But if these fields do not reinforce each other and the standards for evaluating the contradictory information (for example, innocuous social media posts) are not clearly delineated in the algorithmic rule, then it can reduce the accuracy of the algorithm by introducing false-negative error in the "suspicion" assessment.

includes automated analysis and human review and has a margin of error at 2.54 percent.<sup>33</sup> While this may first appear to be trivial, in practical effect it would mean nearly half a million visitors to the U.S. were denied a visa waiver, subject to significant additional scrutiny, and potentially deterred from visiting the U.S. every year. The combined effect of more error and more human review will result in substantial additional labor costs, which are not reflected in the DHS's estimated cost to the public of \$265 million for the ESTA program proposal.<sup>34</sup>

\* \* \*

DHS's proposal to collect the online identifiers of travelers under the Visa Waiver Program is highly invasive and will chill free expression online, will disproportionately affect Muslim and Arab communities within and outside the U.S., will lead to reciprocal burdens for Americans travelling abroad, and will be ineffective and prohibitively expensive. We urge DHS to withdraw the proposal.

Respectfully submitted,

Nuala O'Connor  
Emma Llansó  
Rita Cant  
Greg Nojeim  
Michelle De Mooy  
Joseph Lorenzo Hall  
Aislinn Klos  
Apratim Vidyarthi

Center for Democracy & Technology

---

<sup>33</sup> J.M. Berger & Jonathon Morgan, The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter 46, Brookings Inst., March 2015, [http://www.brookings.edu/~media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis\\_twitter\\_census\\_berger\\_morgan.pdf](http://www.brookings.edu/~media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf).

<sup>34</sup> See Federal Register Notice, *supra* n.1. Under the Paperwork Reduction Act, annual cost burden estimates do not include labor cost for the estimated burden-hours for a proposal. U.S. Office of Personnel and Management, Paperwork Reduction Act Guide 2.0, 39, OPM.gov (April 2011), available at <https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf>.

**Comments on the Customs and Border Protection Bureau (USCBP) Notice: [Agency Information Collection Activities: Arrival and Departure Record \(Forms I-94 and I-94W\) and Electronic System for Travel Authorization](#)**

**Pages 1-5**

-----  
Comment Submitted by Smita V

Comment

View document:

I think this will be a grave invasion of privacy. Including it in a form at the customs will scare people into not expressing their thoughts on their social media pages, which is a serious barrier to freedom of speech and expression. There will be pressure from the state to conform to what the state thinks is right or patriotic, which is not how a democracy should function.

-----  
Comment Submitted by B Van Meter

Comment

View document:

apparently amendment 4 is just filler text these days. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. THIS IS CONSIDERED UNREASONABLE SEARCHES.

-----  
Comment Submitted by Robert Miles

Comment

View document:

Sounds like 1984 to me

-----  
Comment Submitted by Ludo Van son

Comment

View document:

Bad idea for creatING a freelance world

---

Comment Submitted by Christopher Miller

Comment

[View document:](#)

It's none of your business.

---

Comment Submitted by Harry Jones

Comment

[View document:](#)

Terrible idea, and not of any valid use.

---

Comment Submitted by Doris Woolf

Comment

[View document:](#)

stp digging it drives me bananas

---

Comment Submitted by J.B. Van Wely

Comment

[View document:](#)

Unconstitutional, unjustified, waste of taxpayers' money

---

Comment Submitted by Filipescu Mircea Alexandru

Comment

[View document:](#)

One of the most ludicrous legal proposals to have hit the modern world. Authorities should have no business with what people do online, especially if they aren't doing anything illegal! Please keep the internet on the internet, and real life in real life... mixing the two beyond a certain point is neither a rational nor a productive act. Thank you.

---

Comment Submitted by Zoe Humphreys

Comment

[View document:](#)

I think this is a gross invasion of privacy and attacks freedom of speech.

---

Comment Submitted by Daniel Joyce

Comment

[View document:](#)

This is such a waste of money and would be completely ineffective. If someone planned to do harm they could cultivate and spread not only a benign pressence but even offer misinformation and false leads. This is an infantile approach to national security, a gross violation of our rights, and impossible to implement without bias. Governments spy on their enemies in order to keep its people safe. More and more I realize that the government considers its own citizens its enemy.

---

Comment Submitted by Amber Wright

Comment

[View document:](#)

This is invasive and unnecessary. The government has no business doing this and should be ashamed. I do not want my social media up for inspection by the FBI or anyone else unless I am under suspicion of a crime and a warrant has been obtained.

---

Comment Submitted by Neil Vaneerde

Comment

[View document:](#)

Stay out of our files.

---

Comment Submitted by Martin O'Sullivan

Comment

[View document:](#)

This is a step too far. And stifles speech.

---



Comment Submitted by Robert McAuliffe

Comment

View document:

This is a blatant over-reach equivalent to requiring all bedrooms be bugged before entry to the US is allowed. That would not be acceptable and this should not be too.

---

Comment Submitted by Cliff Mitchell

Comment

View document:

This is completely unnecessary and totally unacceptable.

---

Comment Submitted by William Hurless

Comment

View document:

Its sad that you are allowing fear destroy freedom and privacy.

---

Comment Submitted by Rob Juneau

Comment

View document:

Desperate, paranoid heavy-handedness like this only feeds the problem. Better laws need less regulation. Please wake up soon. Thanks.

---

Comment Submitted by Vic Wu

Comment

View document:

This is a serious waste of money , time and effort. If anything - it sounds like a plan to pay a company that is politically connected to consult and therefore, waste taxpayer funds.

---

Comment Submitted by Simeon Vasilev

Comment

View document:

Social media allows one to juggle a wide array of online identities, some of which bordering on the ridiculous or completely fictional. My opinion is that a lot of the stuff said online can be taken out of context or interpreted in a damaging manner to the passenger. Moreover, analysis of social media opens the flood-gates to thought-policing and can severely impair free-speech and the work of activists.

---

Comment Submitted by Peter Lugerbauer

Comment

View document:

That would be real paranoia!

---

Comment Submitted by Julie Owono

Comment

View document:

It would be an illegal, disproportionnate, unnecessary violation of my privacy.

---

Comment Submitted by Martin Nicolaus

Comment

View document:

It sucks

---

Comment Submitted by Adrian McCarthy

Comment

View document:

This would have a chilling effect on personal communication and expression, harming democracy and the marketplace of ideas. It's far too difficult to define social media to even know where the bounds of someone's requirements to report about there presence lies. Are vanity website social networks? Instant messaging friend lists? Personal email servers?

---

Comment Submitted by Richard Moats

Comment

View document:

Surveillance absent reasonable suspicion is un-American, ineffective, reveals us as irrationally fearful and reactionary.

---

Comment Submitted by Barb Quarton

Comment

View document:

Another blunt example of the USA having become a totalitarian state.

---

Comment Submitted by Mark James

Comment

View document:

It's an invasion of privacy.

---

Comment Submitted by Gage Hutchins

Comment

View document:

This is a terrible and invasive idea, and should never be put into action. The NSA already illicitly collects all this information and more, why should taxpayers pay millions of dollars for redundant data-harvesting? Especially when there's already so much information in the system that it's impeding investigations more than helping!

If you do this, you'll just give intelligent people yet another reason to NOT want to come to this country. It's hard to run high-tech companies (Google, Microsoft, Apple, Pixar, etc.) and other advanced industries (e.g. medical) without lots of highly educated people. Thus, this plan would have long-term harm on America at social, political, health, educational, AND economic levels. It almost seems like you're TRYING to ruin our country!

---

Comment Submitted by Anonymous

Comment

[View document:](#)

The US government will successfully demand I surrender keys to social media account over my quite literally dead body. I am willing to accept a contempt ruling on this issue. I am quite willing to go to court over this issue.

---

Comment Submitted by Ian Woolf

Comment

[View document:](#)

For a nation that claims to value freedom, its appalling that you plan to destroy those same freedoms. You want to punish people for what they liked on facebook or complained about on twitter? No freedom of speech for foreigners, eh? They don't count as men with rights in the constitution?

---

Comment Submitted by Jack Roberts

Comment

[View document:](#)

I think it's way over the top. If there is just cause, that's a different matter. That's what search warrants are for.

---

Comment Submitted by Scott Koterbay

Comment

[View document:](#)

This is idiotic and insulting.

---

Comment Submitted by Shubham Yogi

Comment

[View document:](#)

I don't want to fret about creating an online persona to enter the US, just because I might be screened further for security purposes if I do not have an online presence. The customs can check the records maintained by the country of origin of travellers.

---

Comment Submitted by Linda Vasquez

Comment

View document:

No United States Citizen should be subjected to a social media search unless there is a warrant issued by a judge for that purpose or a crime is in progress by that person. Regarding people traveling here who are Not US Citizens then a search can be conducted, however, strict freedom of speech guidelines vs criminal associations should be followed regarding decisions to enter USA.

---

Comment Submitted by William Mabury

Comment

View document:

This is an ill advised and frankly fascist proposal to determine if people are guilty of thoughtcrime according to the standards of whomever the current regime is. Also, sifting through terabytes of random social media data will only make it more difficult to discover real threats.

---

Comment Submitted by Suzanne Saunders

Comment

View document:

This is a waste of money -- how many real terrorists would make public posts?

---

Comment Submitted by Gordon Parker III

Comment

View document:

This is an absolutely egregious, unnecessary and unconstitutional invasion of privacy and person and is totally unacceptable.

---

Comment Submitted by Ronald Norman

Comment

View document:

It sucks and it illegal.

---

Comment Submitted by Kim McCarthy

Comment

View document:

This is a witch hunt, very much like drug tests for welfare benefits. So much wasted money for so little results. Feed the hungry, house the homeless, save the whales. Just stop throwing money away.

---

Comment Submitted by Rebecca Kimsey

Comment

View document:

This is unwarranted search, and is barred by the US Constitution. I am not about to give up my rights, for any reason. Such an invasion of privacy of all travellers will serve no reasonable purpose, other than to give governments far too much access into the privacy of its citizens.

---

Comment Submitted by Shea Molloy

Comment

View document:

I think that will fundamentally change the way people think and speak out about things while failing to actually help reduce violence or acts of terrorism.

---

Comment Submitted by Kris Ramsden

Comment

View document:

It's a gross violation of privacy, it denies the human right to freedom of speech and association. It's one more step towards a fascist authoritarian society which wants to control everything and everyone. There's going to be big trouble as people become more aware of what's being attempted.

---

Comment Submitted by Per M. Jensen

Comment

View document:

By behaving in a morally inferior way you are not protecting your country from terrorist attacks but encouraging them.

---

Comment Submitted by Bill Lindner

Comment

View document:

It's time to rethink this fraudulent War on Terror that keeps being used against law-abiding US citizens. Unless you're actually a suspected terrorist, your info should be off limits.

---

Comment Submitted by Bogdan- Gheorghe Iorga

Comment

View document:

Is OK

---

Comment Submitted by Michael Lederman

Comment

View document:

I think it's a great idea

---

Comment Submitted by Dan Gabriel Stoica

Comment

View document:

Some of information should be used to prevent any crime but some informations must be private and confidential.

---

Comment Submitted by Max Kaehn

Comment

View document:

Publicly available information is publicly available and is fair game. Be mindful of the Fourth Amendment and of false positives; government should be liable if they make a mistake and conflate one person with another

---

Comment Submitted by Keith Woolsey

Comment

View document:

Would not visit USA if this gets in. Bye bye tourist dollars

---

Comment Submitted by Mariu Suarez

Comment

View document:

We have a right to privacy from government surveillance. PRIVACY RIGHTS!

---

Comment Submitted by Matias Rocha

Comment

View document:

What I want to say uses too many expletives for polite conversation, but you can guess how I feel. Drop dead, Totalitarianism. I want the old USA back, the one that at least tried to act like a democracy. You're an embarrassment to your neighbors up north, and a bad example for governments everywhere, who take your example as an excuse to crack down on the freedoms your nation was founded to protect.

---

Comment Submitted by Elizabeth Krijgsman

Comment

View document:



Do the words unwarranted search and seizure have any meaning to the clowns who thought this up?

-----

Comment Submitted by Alexander Zimering

Comment

View document:

hope they like my porn and also see that i'm not a terrorist

-----

Comment Submitted by Wilfried Vetter

Comment

View document:

Please respect privacy

-----

Comment Submitted by Christopher Pelham

Comment

View document:

Why they would want to do so is understandable, but given how many, many times the US government has used surveillance for political goals, eg surveilling MLK and so many peaceful activist movements, I can't trust the Feds to use this responsibly. And I can't trust them to distinguish between innocent conversation and actual threats. I think it is much better to encourage us citizens to voluntarily report instances of threatening speech or allegiance to terrorist groups etc if and when we see it online. Also, there are far far more instances of hate speech by white American citizens than there are foreign terrorists entering our country and those are a much bigger concern yet the govt seems to largely ignore them.

-----

Comment Submitted by Harry Knowles

Comment

View document:

Would deter me from visiting the US again. I barely use social media but this is a privacy issue which impinges on a person's right to privacy. So unless they can establish at law there are grounds to search an individual's online presence they should not be given access. The message Homeland

Security is sending here is that everyone entering the US is a suspect unless it can establish otherwise. This is not the sign of a healthy democracy.

---

Comment Submitted by Richard Magerkurth

Comment

View document:

I feel that this proposed idea is a gross violation of our rights to peaceably assemble and to be free from unreasonable searches and seizures.

---

Comment Submitted by Jerry Sawyer

Comment

View document:

Invasion of my privacy. 1984 come true. So much for our constitution.

---

Comment Submitted by Karl Koscher

Comment

View document:

Due to the length of my comments, please see the attached document in opposition of the proposed change.

Attachment Contents:

U.S. Customs and Border Protection (CBP) should not implement the proposed change. The proposed change is overly burdensome, overly vague, and ineffective, as detailed below.

The proposed change adds an optional question to I-94, I-94W, and ESTA asking for social media identifiers. While not explicitly spelled out in the request for comments, ostensibly the purpose of this change is to exclude aliens who spread unprotected terrorist propaganda on social media networks. While I think we can all agree that these people should be excluded from entering the U.S., asking millions of visitors for their social media identifiers is not an effective way to enact this policy.

First, the question itself ("Please enter information associated with your online presence—Provider/Platform—Social media identifier.") is overly vague. What counts as a social media platform? Sites such as Facebook and Twitter are obviously social media platforms, but what about sites like Flickr? Does Google+ count if you "upgraded" your Google account but never posted anything? Are forums social media platforms? How about online games and networks such as Xbox

Live? Do sites that accept comments constitute a social media platform, such as newspapers or even the TSA Blog? What about sites that accept customer reviews, such as Amazon? People have numerous online identities, and it's not clear which CBP is interested in. If the answer is "all," then the response is unreasonably burdensome. Can you remember every username you used on every site you ever visited? If you exclude certain sites because you don't consider them to be a "social media platform," will this lead CBP to accuse you of intentionally hiding or omitting information? The only safe option appears to be declining to answer at all, which defeats the purpose of the question in the first place.

One potential fix is to only list the social media platforms that CBP cares about and ask for those identifiers. However, this does not seem like a feasible option. The social media ecosystem is highly dynamic, and any list will surely be out of date as soon as the forms are made. As a dramatic example of this, see xkcd's 2007 map of online communities (<https://xkcd.com/256/>). At the time, Facebook is smaller than LiveJournal, while MySpace dominates. Even the more recent 2010 map (<https://xkcd.com/802/>) shows large communities that have largely become irrelevant, such as Farmville. Furthermore, not everyone has an account on major social media sites like Facebook. I never had a MySpace account. My boss does not have a Facebook account. Would not listing a Facebook account be suspicious in the eyes of CBP?

Whereas some people may have no social media presence, others may have multiple accounts on the same service. For example, I have a primary Twitter account, a few parody accounts, an account that tweets absurd legalese from contracts I've seen, and control over other shared accounts, including those for a college radio station, a phone company parody, and a cryptography and privacy advocacy group. Does CBP expect me to list all of my personal accounts? What about accounts that are shared? If shared accounts are requested, what impact will they have on the vetting process?

Viewing someone's social media presence as part of a vetting process for admitting an alien into the United States would be ineffective. Due to the privacy settings provided by several social media platforms, CBP may be unable to determine anything about a particular account. For example, if one protects their Twitter account, third parties who do not follow that account are unable to see any

tweets they have made or even who they follow. Facebook provides even more fine-grained privacy options.

Is CBP only interested in people spreading terrorist propaganda, or will those following certain accounts also be excluded? Not everyone following terrorist propaganda accounts is looking to be indoctrinated; for example, some may be academics studying how terrorists use social media. Excluding people for seeking out (but not spreading) certain speech seems to raise First Amendment concerns. Furthermore, due to the aforementioned privacy controls, CBP may not be able to identify if an account follows other accounts of interest, limiting the effectiveness of the proposed change.

Additionally, social media identifiers (which I will call usernames) are often aliases to underlying account identifiers. For example, one can change your Twitter username at any time while still having the same underlying account. What are the consequences if someone changes their

username after entering it on the I-94/I-94W/ESTA? What if their old username is taken over by someone spreading terrorist propaganda? Since ESTA authorizations are valid for two years, there is a real risk of social media identifiers becoming outdated, or suddenly belonging to a different person.

On some platforms, usernames are optional. For example, on Google+, I am only searchable by my full name. While my name is relatively unique, CBP would be unable to identify the social media presence of people with common names. These social media platforms rely on network effects of human interaction – if I knew someone named David Smith I could likely find him because at least some of my other contacts know him, so the social media platform would rank his profile highly – but CBP officers would likely not be close in David Smith’s social graph, preventing them from finding that particular David Smith among all the others.

Some platforms have the ability to use an internal ID instead of a username. For example, while I have no Google+ username, you can find my Google+ profile at <https://plus.google.com/112570544857847727022>, or my Facebook profile at <https://www.facebook.com/profile.php?id=10709870>. But how many travelers have the technical savvy to discover these identifiers, let alone remember them when presented with an I-94 form. It should be obvious that asking for these social media identifiers is overly burdensome.

Finally, it should be noted that many immigration controls are done on a reciprocal basis. For example, when CBP began collecting fingerprints under US-VISIT, several other countries began to collect fingerprints of Americans (and only Americans). If CBP begins collecting visitors’ social media identifiers, we should expect other countries to collect Americans’ social media identifiers. These countries may not have the same free speech protections we have, and may imperil those who have inadvertently violated the speech laws of countries they are visiting by simply posting content on social media platforms while in the U.S.

In conclusion, the additional question -- “Please enter information associated with your online presence—Provider/Platform—Social media identifier.” – is overly vague, overly burdensome, and an ineffective means for carrying out U.S. immigration policy, and should not be added to the I-94, I-94W, or ESTA.

---

Comment Submitted by Kenneth Murphy

Comment

View document:

I think it's a terrible waste of money. What's to stop a criminal or terrorist from making a fake account to give to the authorities?

---

Comment Submitted by Maxine Kaufman- Lacusta

Comment

View document:

The US is a beautiful country with lots of great people and Amtrak! But if this provision were added, I would likely stop visiting. The idea that I and/or my social media contacts and theirs on down the line might be endangered because someone powertripping border official is having a bad day is as creepy as placing small children or babies on the no-fly list for sharing a name with someone the government is suspicious of.

Please stop and think before adding additional measures characteristic of a police state!

-----

Comment Submitted by Tony Patrick

Comment

View document:

Identity can't flourish without privacy.

-----

Comment Submitted by Mats [Last Name Unknown]

Comment

View document:

while it may appear to be a sound proposition, any social media analytics are only likely to cause false positives as well as false negatives in varying proportion to a subcultures relevant traits.

an example of this would be scientifically literate subgroups facing suspicions for mentioning chemicals which could, in addition to their intended use, be components in chemical weapons.

another example would be those who play games, often involving military strategies, conflicts, clans, cults, attacks, missions and so on.

yet more examples would include any subgroup which uses sarcasm, jokes or politically insensitive expression to cope, diffuse, reason or argue any particular event in a way that, to any analytical algorithms unaware of social context or conversational clues would determine to be sympathetic to the enemy when they are in fact subverting their influences with humor

-----

Comment Submitted by MelvinTtaylor

Comment

View document:

First off, you would be wasting good tax payers money on me or mine, we have done all the traveling while in the military, we do not desire to travel, even across the country. I am into gaming

only, now if that a concern, that I am a better player, than spend the money to find out, other wise, GO after the one who would make mine and my families live a problem, not us!

---

Comment Submitted by Maureen O'Brien

Comment

View document:

No. I think is unreasonable search and seizure plus a waste of taxpayer money. I also believe the data won't be secure and may be sold off to the highest bidder.

---

Comment Submitted by Robert McCormack

Comment

View document:

an absolute disgrace! privacy invasion is already far beyond the boundaries of reasonableness & the benefits are subjective at best..We need far LESS invasion & much more respect for personal privacy

---

Comment Submitted by Chris King

Comment

View document:

Demanding access to my social media profiles and posts, when I have been accused of no crime, is an unwarranted and unnecessary intrusion into my private communications. Surely anyone who is a legitimate threat to the US is either not going to provide accurate access information, &/or will delete potentially incriminating posts and contacts beforehand. The rest of us should not be subject to such sweeping US government searches, and retention, of our social media interactions for no good cause - it is invasive, chilling and furthermore likely to be extremely ineffective.

---

Comment Submitted by Holger L. Ratzel

Comment

View document:

I think the U.S.D.o.H.S. should not suspect everybody to be a terrorist. They should realize that requesting this information will result in a hay stack that is to big to search. It's classic example of TMI, that will create a lot of false positive and not detect one true terrorist. They should just look at <[https://en.wikipedia.org/wiki/Evaluation\\_of\\_binary\\_classifiers](https://en.wikipedia.org/wiki/Evaluation_of_binary_classifiers)> and should be able to realize that the number of terrorists is to low compared to the number of persons entering the U.S. to produce

meaningful results, regardless of how much information is collected on every traveler. And by the way: The risk of being killed by a U.S. inhabitant with a gun is far bigger than the risk of being killed by a terrorist with a bomb.

---

Comment Submitted by Hein Moritz

Comment

View document:

If they want the information, a warrant should be applied for.

---

Comment Submitted by Paul te Vaanholt

Comment

View document:

Social media posts are often not serious and can easily be misunderstood. Especially underage people do not see consequences of their online behavior (this is a biological fact). One could say that 'responsible social media use' would be common sense, but common sense is not common. Yes, when one looks at a social media account from a terrorist one might see info - in hindsight - but that does not mean that every stupid post leads to a terrorist or even suspect. Let alone stupid posts of friends or friends of friends.

Also, this kind of scanning would be fairly easy to trick, by simply creating a second one to hand over.

Btw, I do not use soc media myself (except for LinkedIn, which is hardly social), so personally I don't care much. But this is yet another case of a government trying to over-police, with a technically and/or socially impossible/improper measure.

---

Comment Submitted by Susan Rautine

Comment

View document:

If they are scanning everything we say and write that is online, they have the information they need. What is the purpose of these invasive methods? What is the reason for spending all the money that could be helping Americans to get off the streets and into jobs.

---

Comment Submitted by Mark Oxner



Comment

[View document:](#)

DHS is welcome to look at my social media presence, just like anyone. But my reentry into my own country, which supposedly has freedom of speech, shouldn't be dependent on examining my social media presence.

---

Comment Submitted by Miranda Rutherford

Comment

[View document:](#)

This idea is costly, inefficient, and potentially could violate the First Amendment by chilling free speech and association. It is not an appropriate procedure for the DHS to investigate.

---

Comment Submitted by Jeffery Wickel

Comment

[View document:](#)

This proposal seems a massive waste of money for an invasive intrusion into personal lives, to unclear purposes. Try to be less Orwellian.

---

Comment Submitted by Esther Jones

Comment

[View document:](#)

I think it's a terrible idea. What I post on social media is not the US government's business.

---

Comment Submitted by John Jack

Comment

[View document:](#)

My online presence is none of your business, thank you very much.

---

Comment Submitted by Lauren Sorensen

Comment

View document:

Please stop this. You have wasted enough taxpayer time and expense with the ridiculously inefficient and ineffective security theater that we all have to tap dance through as it is. Just stop.

---

Comment Submitted by Eric Lindsay

Comment

View document:

Changes to USA intrusiveness via Homeland Security after 9/11 have changed my travel patterns. I formerly visited friends in the USA as a tourist once or twice a year. If I am going to be treated like a terrorist, I will continue my present pattern of visiting countries more friendly to tourism. Visited Norway this year. Canada, Greenland and Iceland last year. Visited Europe previous year. Visited Russia, Mongolia year before that. I am not sure if the tourism dollar is worth much to the USA, but USA has lost me.

P.S. Due to privacy concerns, I avoid Facebook, Instagram, LinkedIn anyhow.

---

Comment Submitted by E M

Comment

View document:

This is pretty damn idiotic for an enormous number of reasons. Let's start with: if you're a terrorist, are you going to give them the real accounts or fake accounts, or maybe just omit that one email address you use for terrorist stuff. How is this supposed to keep anyone safer?

...not to mention the huge potential for mis-analysis and use of content for non-national security judgements (TSA agents are eyeballing enough of people's private lives/stuff already).

....beyond all that, I have a hard time believing the NSA isn't doing this anyway. But at least it isn't asking/requiring people to give their own information up. This might even be a 5th amendment issue, although wiser folks than I would need to weigh in.

But overall: really stupid overreach. Customs enforcement is not justification for playing Big Brother. We're smarter than that.

---

Comment Submitted by Wolter van den Brink

Comment

View document:

The harm done by preventing terrorist actions is a lot greater then the harm done by any terrorist act. Both economical as well as social.

---

Comment Submitted by Joel Iwashige

Comment

View document:

This is an intrusive and intimidating violation of privacy.

---

Comment Submitted by Carl Knudson

Comment

View document:

It seems like a violation of the fourth amendment's protection from unreasonable search and seizure.

---

Comment Submitted by Peter Lee

Comment

View document:

No go.

---

Comment Submitted by Brian Stokes

Comment

View document:

This is draconian, akin to the Nazi Stasi group spying on everyone in Germany, and their private conversations. This kind of authoritarian information gathering has never stopped a terrorist, but has always been abused to punish people. Go after people when they commit crimes, not before. See the movie The Lives of Others. We are not Nazis.

---

Comment Submitted by Wilfried Kaeufler

Comment

View document:

It's silly, stupid, arrogance and unsocial.

---

Comment Submitted by Ivan Zhyvolup

Comment

View document:

This is creepy and inappropriate.

---

Comment Submitted by Gunjar Sutherland

Comment

View document:

I'm shocked, now I know one of many reasons why I don't use social media. I don't want Big Brother looking over my shoulder.

---

Comment Submitted by Pete Powell

Comment

View document:

if you have something to hide, I don't want you entering our country

we have no problem sharing this information and anyone who does may need to rethink their behavior and associations, of course that's part of the trouble with the country now...

---

Comment Submitted by Peter Row

Comment

View document:

All persons, but especially U.S. Citizens, have the right to be free from unreasonable search and seizure. Searching anything that requires a password or other authentication process should require a warrant.

---

Comment Submitted by Adrian Rogers

Comment

View document:

Unless Homeland Security has clear evidence that someone entering the US has definite links to a terrorist organization, their online presence--if they have one, should not be scrutinized.

---

Comment Submitted by MC Kubiak

Comment

View document:

Smells of a police state, not the United States of America.

---

Comment Submitted by Bakota [Last Name Unknown]

Comment

View document:

1984

---

Comment Submitted by Lydia Lacy Wallace

Comment

View document:

This is a breach of individual privacy and will do absolutely nothing to keep us more secure. This sets a dangerous precedence for not only potential immigrants, but also to US citizens and our right to free speech.

---

Comment Submitted by Eric Meyer

Comment

View document:

Not their business!!!!

---

Comment Submitted by Omno Pels

Comment

View document:

One of the most fundamental principles in a society that purports to apply the rule of law is, that one is innocent until proven guilty. This implies that whatever one does in his/her private life cannot be legally accessible to any officer of law until there is sufficient reason to believe that this person is involved in illegal activities or has the intent of such activities. It goes without saying that being on any type of social media is no reason for such a belief. The reverse side of this argument is, that any government that violates this implication no longer applies the rule of law. This means said government endorses lawlessness, meaning it is no longer a legal government, regardless of the fact that it is democratically elected.

---

Comment Submitted by Chris Stuart

Comment

View document:

A country that actually believes in the First Amendment should not spend time, money, and effort trying to find thoughtcrime.

---

Comment Submitted by Zora L. Kolkey, MFT

Comment

View document:

It's unconstitutional and none of your business!

---

Comment Submitted by Raefe Mahadeo

Comment

View document:

This sounds like it needs 500 pages, minimum, of red tape to avoid violating citizens & denizens civil liberties.

Its not on the whole unreasonable to safeguard against threats so long as there's a clear line to prevent witch hunts and the misuse of the information after its been given

---

Comment Submitted by Robert Pennoyer

Comment

View document:

Combing social media data is a terrible way to catch actual bad guys and a very good way to mistakenly incriminate good guys.

---

Comment Submitted by Ken McGlothlen

Comment

View document:

Have you folks even *\*heard\** of the First, Fourth and Fifth Amendments?

---

Comment Submitted by Fred Robel

Comment

View document:

NO. The U.S. DHS should not be allowed to check my social media, or even ask if they can, when I am entering the country. I feel that that would be wrong, and would stifle social media interactions, which are increasingly important for people to have honest discussions about things. Sometimes subjects that may cause a government agency to raise an eyebrow, which is not ok to have to worry about.

---

Comment Submitted by Kelly Schneider

Comment

View document:

This plan is a waste of taxpayer dollars. It is inconceivable that any information gleaned from these activities could possibly be worth the amount proposed to be spent.

---

Comment Submitted by Janice Muller

Comment

View document:

Searching someone's online presence is like going through everyone's garage can. Access to personal information should be accompanied by a warrant based on a reasonable need to search per the US Constitution.

---

Comment Submitted by Alice Shields



Comment

[View document:](#)

I think that plan is unconstitutional, and an outrage to American citizens.

---

Comment Submitted by Aubrey Warsop

Comment

[View document:](#)

It is absolutely absurd to think it will be an effective way to combat threats. Nothing but busy work with the illusion of being helpful.

---

Comment Submitted by Christian Rosager

Comment

[View document:](#)

If it can improve the security I think social media information should be accessible, though I can't see how it would be possible to judge a person based on pure media. Which is why appealing to the decision should be possible

---

Comment Submitted by Heidi Reyes

Comment

[View document:](#)

This is a very bad idea! The people who want to harm the US won't be publishing their plans on their social media profiles. In addition, the posts of people who want to visit the US and the comments on those posts will be scrutinized by the CBP, making it likely that potential visitors and all their friends will censor their online speech.

---

Comment Submitted by Amanda Wintcher

Comment

[View document:](#)

This is a serious overstep. If a person is already known to law enforcement, then that is one thing; but trawling through the social media accounts of every traveller is not only a waste of money and unlikely to find anything useful, but it is also wide open to abuse and misinterpretation of innocent remarks. It also raises the possibility that a person's protected free speech could be used to deny

them lawful entry if that speech happened to contradict the views of local and national government, or those of the person performing the screening.

---

Comment Submitted by Celeste Mattingly, LCSW

Comment

View document:

A horrible violation of our rights to privacy.

---

Comment Submitted by Urvi Nagrani

Comment

View document:

I'm strongly against this program which is unreasonable intrusion into the private social spaces we all inhabit. Even if the account holder opts in, their friends may not wish to surrender their privacy, and collecting their posts violates the spirit in which this information was saved. If the government wants to track public information or posts, fine - but social media accounts are not such pieces of information and should be treated with the same respect and privacy as individual homes.

---

Comment Submitted by Charles Wolfe

Comment

View document:

Customs should need a court order to scan such account of citizens. Immigrants have already been vetted, so why scan again. Visitors are vetted when they apply for a visa so why scan again? Such viewing/examining may be proper when vetting potential immigrants and those applying for a visa. BUT, scanning only when initial examination shows some reason to suspect the person and there should be a need for higher ups signatures authorizing it. I remember the Nixon years and do not want to see them repeated in any fashion.

---

Comment Submitted by Ken Reed

Comment

View document:

It is evil, it is none of the governments business, and as electronic data is easily tampered with, it should never be allowed to stand up to any legal process, without supporting evidence

---

Comment Submitted by Bart Samwel

Comment

View document:

Giving the US government access to my private communications would be reason for me to avoid visiting the US. I think would be is a gross invasion of my privacy and completely inappropriate.

---

Comment Submitted by Nico Keilman

Comment

View document:

As long as you do not have any concrete evidence that I have violated the law, you should not do this.

---

Comment Submitted by Gene Lawson

Comment

View document:

George Orwell's 1984 is that where we are now? We have been there for a long time but they just kept it secret. Don't go public with it! Then we will be more afraid. Isn't that the point?

---

Comment Submitted by Janet Patterson

Comment

View document:

I think this plan is terrifying.

---

Comment Submitted by Sophia Cope, Electronic Frontier Foundation

Comment

View document:

Please see the attached PDF.

Attachment Contents (available at <https://www.regulations.gov/document?D=USCBP-2007-0102-0596>):

August 22, 2016

**VIA REGULATIONS.GOV**

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

***RE: Electronic Frontier Foundation Comments on Proposed Collection of Social Media Identifiers Via Electronic System for Travel Authorization (ESTA) and Form I-94W for Visa Waiver Program Visitors to the United States***  
***Docket No. USCBP-2007-0102***  
***OMB No. 1651-0111***

To Whom It May Concern:

The Electronic Frontier Foundation (EFF)<sup>1</sup> submits these comments to convey our objections to Customs and Border Protection's (CBP) proposal to ask aliens seeking to enter the United States under the Visa Waiver Program (VWP) for their social media handles.

Specifically, CBP proposes to instruct VWP visitors to provide "information associated with your online presence—Provider/Platform—Social media identifier."<sup>2</sup> CBP

asserts that it would be "optional" to provide this information to the U.S. government electronically via the Electronic System for Travel Authorization (ESTA) before embarking

on travel to the U.S. without a visa, or via the I-94W paper form. CBP's goal in seeking this

information would be to provide its parent agency, the Department of Homeland Security,

"greater clarity and visibility to possible nefarious activity and connections" for "vetting purposes." CBP is seeking comments, in part, on "whether the collection of information is

necessary for the proper performance of the functions of the agency, including whether the

information shall have practical utility." We argue that it would not.

**The proposal would be ineffective at protecting homeland security.** CBP's proposal to instruct VWP visitors to disclose their social media identifiers is undoubtedly

<sup>1</sup> EFF is a San Francisco-based, non-profit, member-supported digital rights organization. As recognized

experts focusing on the intersection of civil liberties and technology, EFF actively encourages and challenges industry, government, and the courts to support free expression, privacy, and openness in the information society. Founded in 1990, EFF has over 25,000 dues-paying members.  
2 81 Fed. Reg. 40892 (June 23, 2016), <https://federalregister.gov/a/2016-14848>.

## EFF Comments on CBP Social Media Identifier Proposal

August 19, 2016

Page 2 of 9

backed by a salutary motive to prevent terrorist attacks and other harm to Americans. The

proposal was likely spurred by the discovery after-the-fact that Tashfeen Malik, one of the

San Bernardino shooters, expressed on Facebook her support for the Islamic State group.

Presumably, CBP/DHS would use disclosed social media handles to peruse *publicly* available posts on Facebook, Twitter, Instagram and other social media platforms for evidence of terrorist intentions, affiliations or sympathies, and then deny entry based on

that information. However, Ms. Malik, who was in the U.S. on a fiancée visa, expressed such

sentiments in *private* messages to her Facebook friends.<sup>3</sup> She did not do so in public posts

prior to the attack, according to the FBI.<sup>4</sup> The government would not have access to private

messages and posts by simply knowing applicants' social media handles.<sup>5</sup>

Additionally, when Ms. Malik publicly declared allegiance to ISIS on Facebook after the attack began, she did so under a pseudonymous profile.<sup>6</sup> It is highly unlikely that would-be terrorists seeking to enter the U.S. would disclose their social media identifiers—

whether pseudonymous or using their real names—to CBP that reveal publicly available

posts expressing support for terrorism. It is far more likely that terrorists would create secondary social media profiles that contain benign public posts, and share those handles

when applying to enter the U.S.—or share none at all.

**The proposal contains no standards to ensure that innocent travelers would not be misjudged and denied entry into the U.S.** Even if VWP visitors were to disclose

their actual or primary social media identifiers to CBP, the proposal does not state what standards the government would use to evaluate public social media posts and ensure that

innocent travelers are not denied entry into the U.S. In the past, CBP has taken posts out of

context and misunderstood their meaning. In 2012, for example, Irish national Leigh Van

Bryan was denied entry into the U.S. because he tweeted to a friend: "Free this week, for  
<sup>3</sup> Richard Serrano, "Tashfeen Malik messaged Facebook friends about her support for jihad," *Los Angeles Times* (Dec. 14, 2015), <http://www.latimes.com/local/lanow/la-me-ln-malik-facebook-messages-jihad-20151214-story.html>.

<sup>4</sup> Richard Serrano, "FBI chief: San Bernardino shooters did not publicly promote jihad on social media," *Los Angeles Times* (Dec. 16, 2015), <http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html>.

<sup>5</sup> If public social media posts or other evidence supported probable cause that an account contains evidence of criminal activity, the government could seek a warrant from a judge to obtain private social media messages or other private content stored in the cloud by U.S. providers. *See* 18 U.S.C. § 2703; *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

<sup>6</sup> Tami Abdollah, "Facebook exec says Tashfeen Malik posted ISIS praise during San Bernardino shooting spree," Associated Press (Dec. 4, 2015), [http://www.mercurynews.com/california/ci\\_29202959/facebookexec-says-tashfeen-malik-posted-isis-praise](http://www.mercurynews.com/california/ci_29202959/facebookexec-says-tashfeen-malik-posted-isis-praise); Julia Greenberg, "San Bernardino suspect posted an ISIS pledge to Facebook after shooting began," *Wired* (Dec. 4, 2015), <https://www.wired.com/2015/12/after-sanbernardino-shooting-began-suspect-posted-isis-pledge-to-facebook/>.

## EFF Comments on CBP Social Media Identifier Proposal

August 19, 2016

Page 3 of 9

quick gossip/prep before I go and destroy America."<sup>7</sup> Apparently it was lost on border agents that Mr. Van Bryan was using slang and humor to convey his hope that he would have a good time visiting Los Angeles. It is likely that the government would similarly misconstrue the social media posts of other innocent travelers if they were to provide their social media handles under the proposal.

Additionally, CBP has not explained how the government would avoid using social media posts to exclude individuals who might disagree with American foreign policy but

who have no intention of committing violent acts. The U.S. has a disturbing history of ideological exclusion and the proposal does nothing to ensure that this would not happen in the future.<sup>8</sup>

**The proposal would violate the privacy and freedom of speech of innocent travelers and their American associates.** Universal human rights, long recognized by the

United States and codified in the First and Fourth Amendments, include freedom of speech

and privacy for individuals.<sup>9</sup> Yet CBP's proposal to instruct VWP visitors to disclose their

social media identifiers would intrude upon these fundamental rights.

While unlikely to uncover those with actual malevolent intent, the vague and

overbroad proposal would result in innocent travelers disclosing a whole host of highly personal details. The proposed language confusingly seeks “information associated with your online presence—Provider/Platform—Social media identifier.” Some people would likely interpret this instruction to include all manner of online accounts, far beyond “social media.” Other people may interpret it to include passwords as well as identifiers, enabling the U.S. government to easily access private content. Even if travelers disclose only their social media handles, this can easily lead the government to information about their political leanings, religious affiliations, reading habits, purchase histories, dating preferences, and sexual orientations, among other things. Moreover, given the highly networked nature of social media, the government would also learn such personal details about travelers’ family members, friends, professional colleagues, and other innocent

<sup>7</sup> Kashmir Hill, “Did U.K. Tourists Deported Due To Tweet About ‘Destroying America’ Get Pranked?,” *Forbes* (Jan. 30, 2012), <http://www.forbes.com/sites/kashmirhill/2012/01/30/u-k-tourists-deported-due-to-tweetabout-destroying-america/#16f9f92b32b4>.

<sup>8</sup> See, e.g., Sheldon Chad, “Ramadan’s visa ban lifted,” *The Guardian* (Jan. 23, 2010), <https://www.theguardian.com/commentisfree/belief/2010/jan/23/tariq-ramadan-clinton-visa>; American Association of University Professors, “Administration Will Address Ideological Exclusion” (Jan. 13, 2011), <https://www.aaup.org/AAUP/newsroom/prarchives/2011/ACLUjanlet.htm>.

<sup>9</sup> See Universal Declaration of Human Rights, arts. 12, 19 (Dec. 10, 1948), <http://www.un.org/en/universaldeclaration-human-rights/>. Article 12 states, in part, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence....” Article 19 states, “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

## EFF Comments on CBP Social Media Identifier Proposal

August 19, 2016

Page 4 of 9

associates, many of whom may be U.S. citizens and/or residents with constitutional and statutory rights.

Additionally, CBP’s proposal would chill the free speech of VWP visitors. Unwilling to share such intimate details with CBP, many innocent travelers would engage in selfcensorship,

cutting back on their online activity (or deleting it altogether)<sup>10</sup> out of fear of being wrongly judged by the U.S. government. Visitors may fear that the government would

use this information against them not just during the entry vetting process, but also in other unknown and future contexts. For example, today’s VWP visitors may become



tomorrow's legal permanent residents or naturalized citizens.<sup>11</sup> Or they may forgo visiting the U.S. altogether, impacting their ability to travel, and also preventing the U.S. economy from benefiting from international commerce and tourism.

Importantly, many VWP visitors have legitimate reasons for being pseudonymous online—publicly active but privately unknown—in their home countries. They may be activists or political dissidents who fear being ostracized by their communities, persecuted

by their governments, or even killed for their beliefs and activities.<sup>12</sup> Once VWP visitors disclose their pseudonymous social media identifiers to the U.S. government, those accounts would forever be associated with their real, passport-verified identities. CBP has

not explained how it would protect the online identities of vulnerable travelers, thereby placing their physical safety as well as their privacy and freedom of speech at great risk.

**The proposal is inconsistent with the U.S. government's promotion of Internet freedom around the world.** CBP's proposal to instruct VWP visitors to disclose their social media identifiers—and the attendant risks to privacy, free speech, the ability to travel, and the personal safety of innocent travelers—is inconsistent with the U.S. government's long-standing promotion of global Internet freedom. The U.S., of course, has

<sup>10</sup> See *supra* n. 7. Mr. Van Bryan's experience with CBP inspired him to make his Twitter account private, affecting his ability to engage in public conversations and debates, even in his home country.

<sup>11</sup> Consider the pre-social media case of the "L.A. Eight," where the U.S. government sought to deport two U.S.

residents who exercised their First Amendment right to lobby against the Israeli occupation of Palestine. See

Neil MacFarquhar, "U.S., Stymied 21 Years, Drops Bid to Deport 2 Palestinians," *New York Times* (Nov. 1, 2007), <http://www.nytimes.com/2007/11/01/us/01settle.html>.

<sup>12</sup> See David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of*

*opinion and expression on the use of encryption and anonymity to exercise the rights to freedom of opinion and*

*expression in the digital age*, [A/HRC/29/32] at 3 (May 22, 2015) ("Encryption and anonymity, today's leading

vehicles for online security, provide individuals with a means to protect their privacy, empowering them to

browse, read, develop and share opinions and information without interference and enabling journalists, civil

society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."), <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf>.

EFF Comments on CBP Social Media Identifier Proposal

August 19, 2016

Page 5 of 9

long supported universal human rights.<sup>13</sup> In 2006, former Secretary of State Condoleezza

Rice established the Global Internet Freedom Task Force to focus on human rights and the

Internet specifically.<sup>14</sup> Secretary of State Hillary Clinton gave a sweeping speech on Internet

freedom in 2010.<sup>15</sup> And current Secretary of State John Kerry said in 2015, “We believe people are entitled to the same rights of free expression online as they possess offline.”<sup>16</sup>

The State Department continues to actively promote Internet freedom today.<sup>17</sup>

So it is troubling that another arm of the federal government (CBP, under the Department of Homeland Security) has proposed a policy that would not only undermine

the Internet freedom of innocent visitors to the U.S., but do little or nothing to actually protect Americans from terrorism and other threats to homeland security.

**The proposal is “optional” in name only.** It is unlikely that VWP visitors would view the request for social media identifiers as truly voluntary, thereby exacerbating the

negative impacts on innocent travelers. Rather, innocent travelers would likely feel coerced

to provide such information to the U.S. government and thereby be forced into the impossible choice of abridging their own privacy, engaging in self-censorship, or forgoing

travel to the U.S. altogether.<sup>18</sup> Additionally, CBP has not explained how it would ensure that

border agents do not punish VWP visitors for declining to disclose social media handles, for

example, by extensively interrogating them or otherwise subjecting them to invasive secondary screening.

**The proposal would spur reciprocity by other nations, leading to violations of Americans’ civil liberties overseas.** Should CBP move forward with its proposal to instruct VWP visitors to disclose their social media identifiers, there would surely be a great risk of other governments acting in a similar manner. Other countries may even require that visiting U.S. persons provide detailed information about their online

<sup>13</sup> See, e.g., International Covenant on Civil and Political Rights,

<https://www.congress.gov/treatydocument/>

95th-congress/20 (signed by the U.S. in 1977 and ratified by the Senate in 1992).

<sup>14</sup> U.S. Dept. of State, *Global Internet Freedom Task Force*, Archive (Jan. 20, 2001-Jan. 20, 2009),

<http://2001->

[2009.state.gov/g/drl/lbr/c26696.htm](http://2001-2009.state.gov/g/drl/lbr/c26696.htm).

<sup>15</sup> U.S. Dept. of State, *Remarks of Secretary of State Hillary Rodham Clinton on Internet Freedom*, The Newseum,

Washington, D.C. (Jan. 21, 2010),

<http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>.

<sup>16</sup> U.S. Dept. of State, *Secretary Kerry Delivers a Speech About Internet Freedom and Cybersecurity Before an*

*Audience at Korea University* (May 18, 2015), [http://www.humanrights.gov/dyn/2015/05/secretary-kerrydelivers-](http://www.humanrights.gov/dyn/2015/05/secretary-kerrydelivers-a-speech-about-internet-freedom-and-cybersecurity-before-an-audience-at-korea-university/)

[a-speech-about-internet-freedom-and-cybersecurity-before-an-audience-at-korea-university/](http://www.humanrights.gov/dyn/2015/05/secretary-kerrydelivers-a-speech-about-internet-freedom-and-cybersecurity-before-an-audience-at-korea-university/).

<sup>17</sup> U.S. Dept. of State, Bureau of Democracy, Human Rights and Labor, *Internet Freedom*, HumanRights.gov, <http://www.humanrights.gov/dyn/issues/internet-freedom.html>.

<sup>18</sup> By way of comparison, in 2014, police officers in Illinois often asked individuals during traffic stops for consent to search their vehicles. Even though motorists had a right to refuse, they “consented” 88 percent of the time (21,365 consents out of 24,240 requests). Illinois Department of Transportation, *Illinois Traffic Stop Study, 2014 Annual Report*, at 11, <https://idot.illinois.gov/Assets/uploads/files/Transportation-System/Reports/Safety/Traffic-Stop-Studies/2014/2014%20ITSS%20Executive%20Summary.pdf>.

## EFF Comments on CBP Social Media Identifier Proposal

August 19, 2016

Page 6 of 9

activities.<sup>19</sup> Should CBP ever expand the program beyond visa waiver countries, those with questionable or poor human rights and Internet freedom records would likely be eager to ask the same question of Americans.<sup>20</sup> This would unnecessarily put Americans at risk of being denied entry, or if granted entry, subject to surveillance and excessive scrutiny while traveling abroad.

**The proposal may inspire more serious CBP invasions into the private lives of innocent travelers, including Americans.** CBP’s proposal to instruct VWP visitors to disclose their social media identifiers is just the latest effort in a broader CBP strategy to scrutinize the digital lives of innocent travelers—foreigners and Americans alike—and it

may inspire further CBP violations of privacy and First Amendment rights.

The Department of Homeland Security launched a social media monitoring program in 2010.<sup>21</sup> Two years later, concerned members of the House of Representatives held a hearing<sup>22</sup> where DHS testified that “components of DHS such as U.S. Customs and Border

Protection ... have the authority to engage in law enforcement activities which may include the use of online and Internet materials,” but the testimony did not go into detail about what this means.<sup>23</sup>

Additionally, CBP issued a policy in 2009 related to border searches of electronic *devices* such as cell phones, laptops and cameras possessed by *anyone* entering or leaving

<sup>19</sup> *See, e.g.*, Jane Engle, “Responses abroad to new U.S. entry rules have been low-key,” *Los Angeles Times* (Feb.

22, 2004), <http://articles.latimes.com/2004/feb/22/travel/tr-insider22> (“The principle of reciprocity, which

has long governed visa policies, also discourages over-retaliation. Countries that restrict entry or raise fees

for visitors risk having other countries do the same to their citizens.”); Larry Rohter, “U.S. and Brazil

Fingerprinting: Is It Getting Out of Hand?," *New York Times* (Jan. 10, 2004), <http://www.nytimes.com/2004/01/10/world/us-and-brazil-fingerprinting-is-it-getting-out-of-hand.html>.

<sup>20</sup> See Freedom House, *Freedom on the Net 2015*, <https://freedomhouse.org/report/freedom-net/freedomnet-2015>.

2015. Compare U.S. Dept. of State, *Visa Waiver Program*, <https://travel.state.gov/content/visas/en/visit/visa-waiver-program.html> (South Korea is considered "partly free" in terms of Internet freedom and is also a visa waiver country).

<sup>21</sup> Dept. of Homeland Security, *Privacy Compliance Review of the NOC Publicly Available Social Media Monitoring and Situational Awareness Initiative*, at 1 (May 21, 2015), <https://www.dhs.gov/sites/default/files/publications/privacy-pcr-mmc-7-20150521.pdf>.

<sup>22</sup> House of Representatives, Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence, *Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy* (Feb. 16, 2012), <https://homeland.house.gov/hearing/subcommittee-hearing-dhsmonitoring-social-networking-and-media-enhancing-intelligence/>.

<sup>23</sup> *Written Testimony of Mary Ellen Callahan, Chief Privacy Officer, and Richard Chávez, Director, Office of Operations Coordination and Planning, U.S. Dept. of Homeland Security, for House of Representatives, Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence, Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy*, at 9 (Feb. 16, 2012), <https://homeland.house.gov/files/Testimony-Callahan-Chavez.pdf>. See generally Electronic Privacy Information Center, *EPIC v. Department of Homeland Security: Media Monitoring*, <http://epic.org/foia/epic-vdhs-media-monitoring/>.

## EFF Comments on CBP Social Media Identifier Proposal

August 19, 2016

Page 7 of 9

the U.S.<sup>24</sup> While it might reasonably be assumed that such searches are limited to data that

is on the devices themselves (e.g., photos on a camera or computer hard drive), CBP's policy does not include any limitations on the scope of access.<sup>25</sup> With modern smartphones,

information stored in the "cloud"—on the Internet and not on the device itself—is easily

accessible with a tap of a finger on an "app" icon. As the Supreme Court recently explained,

"Cloud computing is the capacity of Internet-connected devices to display data stored on

remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference."<sup>26</sup>

Should CBP establish a formal policy of instructing VWP visitors to disclose their social media identifiers—which by definition are tied to accounts in the cloud—there surely would be the temptation in the future to expand the scope of *who* is subject to the

policy and/or *what data* is collected or accessed, in addition to making disclosure explicitly mandatory. It would be a series of small steps for CBP to require *all* those seeking to enter the U.S.—both foreign visitors and U.S. citizens and residents returning home—to disclose their social media handles to investigate whether they might have become a threat to homeland security while abroad. Or CBP could subject both foreign visitors and U.S. persons to invasive *device* searches at ports of entry with the intent of easily accessing *any* and *all* cloud content; CBP could then access both public and private online data—not just social media content (e.g., by perusing a smartphone’s Facebook app), but also private communications and sensitive information such as health or financial status.

**Expanding CBP’s “social media” policy to include U.S. persons and/or all cloud content via searches of personal devices at the border would further burden constitutional rights.** The First Amendment right to freedom of speech includes the right

to associational privacy.<sup>27</sup> CBP’s current practice of searching digital devices, even if limited

to data stored on the devices themselves, burdens this freedom of association. It also intrudes upon the First Amendment right to freedom of the press.<sup>28</sup> Unfettered government

access to social media and other communications accounts based in the cloud that include

<sup>24</sup> *CBP Directive No. 3340-049, Border Search of Electronic Devices Containing Information* (Aug. 20, 2009),

[https://www.dhs.gov/sites/default/files/publications/privacy\\_pia\\_cbp\\_laptop.pdf](https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_laptop.pdf).

<sup>25</sup> See *supra* n. 24, § 3.2, Definition of “Electronic Device”: “Includes any devices that may contain information,

such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and

other media players, and any other electronic or digital devices.”

<sup>26</sup> *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).

<sup>27</sup> See, e.g., *NAACP v. Alabama*, 357 U.S. 449 (1958).

<sup>28</sup> CBP recently tried to search the cell phones of a *Wall Street Journal* reporter, a U.S. citizen based in the Middle East who was visiting Los Angeles for a wedding. She advised the agent of her need to protect her confidential sources. See Joseph Cox, “WSJ Reporter: Homeland Security Tried to Take My Phones at the Border,” *Motherboard/Vice* (July 21, 2016), [http://motherboard.vice.com/en\\_uk/read/wsj-reporterhomeland-security-tried-to-take-my-phones-at-the-border](http://motherboard.vice.com/en_uk/read/wsj-reporterhomeland-security-tried-to-take-my-phones-at-the-border).

EFF Comments on CBP Social Media Identifier Proposal

August 19, 2016

Page 8 of 9

detailed records of a traveler’s contacts, both personal and professional, individual and organizational, would exacerbate such First Amendment invasions.

Additionally, courts have held in recent years that the Fourth Amendment, which guards against unreasonable searches and seizures by the government, protects personal

data stored on or accessed via digital devices, including at the border.<sup>29</sup> In so holding, the

courts noted the significant privacy implications of cloud computing.<sup>30</sup> In 2014, the Supreme Court held in *Riley* that a warrant based on probable cause “is generally required

before ... a search [of a cell phone], even when a cell phone is seized incident to arrest.”<sup>31</sup> As

to cloud computing, the Court stated, “To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter... But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a

screen.”<sup>32</sup>

Indeed, the government lawyers in *Riley* “concede[d] that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is,

a search of files stored in the cloud.”<sup>33</sup> Thus, it is troubling that CBP now is seeking access

to some foreign travelers’ cloud-based social media information, at the same time CBP reserves the right to search the digital devices of all travelers, including Americans, without

a warrant or any individualized suspicion.<sup>34</sup>

<sup>29</sup> Under the border search doctrine, searches generally do not require a judge-issued warrant, and “routine”

searches do not require any individualized suspicion (*i.e.*, no probable cause or reasonable suspicion that evidence of a crime will be found). *See, e.g., United States v. Ramsey*, 431 U.S. 606 (1977). However, lower

courts have held that the Fourth Amendment requires that “forensic” computer-aided border searches of digital devices, as opposed to “routine” manual searches, be supported at minimum by reasonable suspicion.

*See United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc); *United States v. Saboonchi* (“*Saboonchi*

*I*”), 990 F. Supp. 2d 536 (D. Md. 2014); *United States v. Kolsuz*, 2016 WL 2658156 (E.D. Va. 2016).

<sup>30</sup> *See, e.g., Cotterman*, 709 F.3d at 965 (“With the ubiquity of cloud computing, the government’s reach into

private data becomes even more problematic.”).

<sup>31</sup> *Riley*, 134 S. Ct. at 2493. *See also United States v. Kim*, 103 F.Supp.3d 32, 55 (D. D.C. 2015)

(discussing *Riley*

at length and stating that the Fourth Amendment analysis “does not turn on the application of an undefined

term like ‘forensic.’”).

<sup>32</sup> *Id.* at 2491.

<sup>33</sup> *Id.*

<sup>34</sup> *See supra* n. 24, § 5.1.2: “In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information encountered at the

border, subject to the requirements and limitations provided herein and applicable law.”

## EFF Comments on CBP Social Media Identifier Proposal

August 19, 2016

Page 9 of 9

\* \* \*

In summary, EFF respectfully recommends that CBP withdraw the present proposal to instruct Visa Waiver Program visitors to disclose their social media identifiers.

Sincerely,

/s/

Sophia Cope

Staff Attorney

Electronic Frontier Foundation

415-436-9333 Ext. 155

sophia@eff.org

---

Comment Submitted by Shawn Mulvihill

Comment

View document:

This is the beginning of the police state. I will not give up my privacy in the name of security! !

---

Comment Submitted by Scott Taylor

Comment

View document:

If it's about protecting our country and our citizens, then we need to use every tool at our disposal.

---

Comment Submitted by Barb Olson

Comment

View document:

None of this should be possible without a specific warrant for a specific person

---

Comment Submitted by Courtney Westcott

Comment

View document:

This is a terrible idea. It's fiscally irresponsible, and a waste of time. Social media is vast and could be under a myriad of different usernames. If this were implemented, it would not surprise me to find people using personal accounts for everything meaningful and professional accounts to give to the U.S. D.H.S. I tend to disapprove of warrant-less searches as well. The premise seems unconstitutional on several levels.

---

Comment Submitted by Laura Anne Welch

Comment

View document:

As a US citizen, I am concerned that in the name of homeland security my rights to free speech and free association as guaranteed by the US Constitution are being compromised and eroded.

---

Comment Submitted by Thomas McCroskey

Comment

View document:

Privacy is important and should be protected. The number of people would are likely to be identified as credible threats to the United States by analyzing their social account activities is very low compared to the excessive invasion of privacy of the large majority of people.

---

Comment Submitted by Gene Ulmer

Comment

View document:

If they want to know my online presence then the US can just go on line and do a search like everybody else

---

Comment Submitted by Jack King

Comment

View document:

I think CPB can ask the question(s) if it's opt-in only. But I would not want Congress to appropriate any funds for this.

---



Comment Submitted by Amanda Papailhau

Comment

View document:

I would finally break my facebook habit cold turkey.

---

Comment Submitted by Paul McCarthy

Comment

View document:

Mind your own damned business! Terrorism and fear-mongering have people worked up about things that cause far fewer casualties than the real killers, like poor health care and medical mistakes.

---

Comment Submitted by Kevin Rhoads

Comment

View document:

Everything I post is public -- even so, none of Uncle Sam's FN business and there should be ZERO tax dollars wasted on this nonsensical invasion of privacy.

---

Comment Submitted by Jason Moultrie

Comment

View document:

Since the dawn of the internet and social media, I have yet to see the basis of anonymity do any real lasting good. The basic tenets of our screening processes should extend to any information that is relatively easy to attain. Social media is a low hanging fruit. Pick it.

---

Comment Submitted by Sean Sheeley

Comment

View document:

This is an invasion of privacy, and a clear violation of the 4th amendment. It shouldn't even be under consideration.

---

Comment Submitted by Mary Therese Virtue OAM

Comment

[View document:](#)

One more invasion! Can any nation justify the cost of this sort of scrutiny?

---

Comment Submitted by T. R. Wilson

Comment

[View document:](#)

No

---

Comment Submitted by Morgan Raven

Comment

[View document:](#)

Private speech must not be used to deny free movement and this speech must not be penalized, period.

---

Comment Submitted by Dimitar Sakarov

Comment

[View document:](#)

This can often be quite misleading, many people treat the social networks as a place for fun and not a serious source of truth where they should be always honest and clear in their statements.

---

Comment Submitted by Sam Moore

Comment

[View document:](#)

My online presence is none of the government's business. Such unwarranted investigation would be invasive, excessive, and intimidating.

---

Comment Submitted by Deb P

Comment

[View document:](#)

This is absurd violation of privacy and a waste of funds. More data is not always better data and this is not a wise or sophisticated use of time or resources.

---

Comment Submitted by Frank Sentell

Comment

[View document:](#)

IT is simply an invasion of privacy and treating you like a crook

---

Comment Submitted by Sian Williams

Comment

[View document:](#)

I think it's ridiculous and awful and a complete invasion of privacy. Yes, the information is publicly available on the internet, it's not truly private. But when strangers see that information on the internet, they don't/can't connect it to me as a real life person. There might be people in China who know things about me I wouldn't tell them face to face...but I don't have to deal with those people, or interact with them. The idea of connecting all that information to my passport is outrageous. And it has the implication/connotation of a government allowing or denying you entry based on you as an individual person, on your personality, your likes and dislikes and friendships. And they shouldn't have the right to do that. My social media presence won't tell you that I'm a danger to your country, it just tells you about my personality, and that's not information I want to give to a government body - it's especially not information I want to hand over to some security guard/checkperson I'm not interested in forging a personal connection with. I am not a US citizen, but I travel to the US to visit family several times a year; why should I have to give a government that isn't even my OWN government more personal information than is already present in my passport?

---

Comment Submitted by Mike Ryan Simonovich

Comment

[View document:](#)

This is a horribly intrusive plan, that will stifle free expression, freedom of assembly, and freedom of conscience. It's patently unAmerican. Don't do it!

---

Comment Submitted by Frank Wilcox

Comment

View document:

We are turning into a police state. Accelerated by fear, mostly by people in Washington and the middle of the country.

---

Comment Submitted by Gary Joseph

Comment

View document:

any person whom is an actual threat will just give dummy account information so why ask

---

Comment Submitted by Sue Jackson

Comment

View document:

No way!!

---

Comment Submitted by John Niendorf

Comment

View document:

You are a disgrace to everything this country stands for. Why don't you try floating this proposal in Iran, Saudi Arabia, or North Korea. It would be a better fit in any of those countries.

---

Comment Submitted by Joel Sparler

Comment

View document:

I understand the need for security, but the concept of security applies to personal considerations as well as national. Corporate interests should be allowed such access only with explicit consent of the person in question; Government entities should be allowed such access only by a court order and probable cause.

---

Comment Submitted by Nathan Shaulis

Comment

[View document:](#)

Surely the DHS already possesses plenty of resources and tools with which to protect our nation.

---

Comment Submitted by Jonathan Peterson

Comment

[View document:](#)

An expensive program to scan social media for terrorist tendencies is not only unamerican, it's incredibly stupid and useless.

---

Comment Submitted by Cory McGregor

Comment

[View document:](#)

I am usually very honest with boarder patrol when I cross the boarder, but in this case I would deny having used social media, just to avoid adding extra inconvenience to an already very inconvenient process.

---

Comment Submitted by Ellen Schrantz

Comment

View document:

See attached file(s)

Attachment Contents (available at: <https://www.regulations.gov/document?D=USCBP-2007-0102-0585>):

### **Internet Association**

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

<sup>1</sup> 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.

-----

Comment Submitted by Jennifer Schmitt

Comment

View document:

Do not do this.

-----

Comment Submitted by Giovanna Salazar

Comment

[View document:](#)

Such program would be a clear violation of privacy and could potentially limit freedom of expression. It's simply outrageous.

---

Comment Submitted by Nikki Little

[Comment](#)

[View document:](#)

If you don't have any actual intel that makes you suspect people, that's your problem, not ours. If you DO have any legitimate queries about an individual, you should be able to get a warrant easily to search someone's social media, but Donny ask us to just hand it over because Patriot Act 'Murica!

---

Comment Submitted by Josef Taylor

[Comment](#)

[View document:](#)

We should be working to open our borders, not close them.

---

Comment Submitted by Loren Stermann

[Comment](#)

[View document:](#)

This is an enormous violation of several articles of the Bill of Rights, and is completely unconscionable. Frankly, it reeks of McCarthyism, and is the exact opposite of what the U.S. should be standing for. Anyone who advocates for such measures should be ashamed of themselves.

---

Comment Submitted by Sue Smith

[Comment](#)

[View document:](#)

Will not bother visiting USA if they go ahead with this.

---

Comment Submitted by Aleksander Laane

[Comment](#)



View document:

You only make chaos stronger. End capitalism, ensure the proper social security system, and the society will prosper, let east be east and west be west, and you will have no terror in no time. Just test.

---

Comment Submitted by M M

Comment

View document:

This is a terrible and dangerous idea.

---

Comment Submitted by Rachel K

Comment

View document:

I think this is a horrible idea and will have a chilling effect on free speech, which is one of the foundations of the United States. I understand the motivation behind the proposed idea, given how terrorist groups are currently using social media, but this is not the right way to go about addressing that issue. I do not think the plan has been carefully thought out and is reactionary, when something like this needs a great amount of consideration. Online text gives very little context and oftentimes the original meaning is lost or misinterpreted, especially in light of cultural differences. This proposal opens the door up for discrimination, misunderstanding, and silencing those who might at times disagree with majority values or beliefs.

---

Comment Submitted by Thomas Lee

Comment

View document:

i think it abhorrent. Mind you, not as bad as some of the things Trump is advocating, but terrible nevertheless.

---

Comment Submitted by Dirk Van nouhuys

Comment

View document:

It disgusts me.

---

Comment Submitted by Janine McNamara

Comment

[View document:](#)

This proposal is insanity - Big Brother to the umpteenth degree!

---

Comment Submitted by David James

Comment

[View document:](#)

This is a bad idea on its face, as much of the 'analysis' will have to be done by computer programs. Even with an excellent program for that purpose, the number of people required to evaluate the items flagged by the program would either A) be huge, and therefore expensive or B) too understaffed and/or overworked to be effective. Add the proposed cost of the program and you've got a boondoggle only a kleptocracy could love.

If you have probable cause to suspect an individual and reason to believe their social media could provide relevant information, do it the right way: get a warrant. If you want to go fishing, which is what this is, grab your rod and license head to your favorite body of water, not your computer.

---

Comment Submitted by Henry Nourse

Comment

[View document:](#)

Such actions would be a highly unfair misuse of people's data as well as a terrible means of deciding if a person should be allowed into the country and an invasion of privacy. Social Media accounts are private matters, they are no business of the state and certainly not border staff. Expenditure on this scale for such a flawed programme is utterly ludicrous and impossible to defend. It is more likely that the innocent would be punished unfairly than it is that those who shouldn't enter the country will be stopped. What's more, how would the scheme cope with multiple social media accounts under one persons name? I personally own 7 accounts, other people may have more, such huge amounts of data could never be properly screened safely and in a timely manner. The threat of such information being given away to other agencies and companies is also unacceptable. If a resident of another nation enters the United States, why should their data be stored on a US database and be available to US authorities? Such a measure is an unacceptable breach of freedom and privacy.

---

Comment Submitted by Anonymous

Comment

[View document:](#)

The Dep't of Homeland Security should be abolished and replaced with an agency that merely coordinates data between legitimate government entities.

---

Comment Submitted by Igor Kolker

Comment

[View document:](#)

The government should not be able to search your social media, email, other digital content at the border. While there can be an argument that your possessions can be searched at the border this should not extend to things not actually on your person even if you have means to access them (cell phone) on your person. The government should not be able to search your house just because you travel with your house keys.

---

Comment Submitted by Michelle Lehr

Comment

[View document:](#)

An unbelievable violation of privacy. And knowing how easy it is to misunderstand or take something out of context when going through social media, this is a scaremongering waste of time, and a reprehensible attempt to control and corral freedom of speech online. Privacy cannot be bulldozed at every turn, not in a nation that prides itself on liberty and justice for all. There is no justice in being considered guilty until a thorough search of personal, private information proves otherwise. There is no liberty in unfettered government surveillance and control of speech through fear. Privacy matters. Government surveillance of private citizens by default is something that belongs in a dystopian novel, not the United States.

---

Comment Submitted by Catherine Stasevich

Comment

[View document:](#)

This is the kind of regulation that leads to the throttling of free speech out of fear of retribution and prosecution. It is as wrong for the government to request social media account snooping as it is for potential employers to request it. We already know that employers discriminate based on what they find by illegally requiring employees to submit social media account information, and there is no doubt that government agencies would illegally discriminate, detain, and imprison innocent people

through unfounded assumptions based on what they find in social media accounts. We are polarizingly political on social media. We exaggerate. We make sarcastic remarks that may not be obvious to those outside our friend groups. We friend people indiscriminately for business and statistics purposes. Government snooping on social media accounts with no justifiable suspicion would surely lead to the infringement of free speech and personal liberty.

---

Comment Submitted by Michael Stolz

Comment

[View document:](#)

This would be a very undemocratic use and invasion of my privacy.

---

Comment Submitted by Peter Kahn

Comment

[View document:](#)

This is an unacceptable intrusion that violates forth amendment rights.

---

Comment Submitted by Jennifer Zornow

Comment

[View document:](#)

I think it's a violation of my First and Fourth amendment rights to have the government collect my data without a warrant.

---

Comment Submitted by Van Swearingen

Comment

[View document:](#)

This would be a pointless waste of time.

---

Comment Submitted by Bonnie Price

Comment

[View document:](#)

Spend the money on better intelligence.

---

Comment Submitted by Janet Rubinoff

Comment

View document:

I am a dual U.S.- Canadian citizen, and I object to any government inquiries into my social media accounts because I live in Canada. As a U.S. citizen (born in New York) I should have the right to enter my country without scrutiny of my social messages to family & friends! It is outrageous!

---

Comment Submitted by Avner Shiloah

Comment

View document:

I believe it's not only an excessive breach of privacy, but also a useless waste of money.

---

Comment Submitted by Pamela A. Lowry

Comment

View document:

The US DHS plan to search our online presence isn't just an unwarranted invasion of privacy, but a ridiculously expensive program. The money would be better spent on educating and feeding our children.

---

Comment Submitted by Matthias Pftzner

Comment

View document:

The U.S. is a country of free speech and prides itself as the country of freedom.

So, live to that standards.

This action of trying to get more control over foreigners is an act against basic human rights, and should therefore not be implemented.

---

Comment Submitted by Lauren McWilliams

Comment

View document:

When the government is allowed to scrutinize personal information as a means of making objective judgements on how fit you are to exist in a country is when we make manhunts and stereotypes the basis for a legal decision. While I am thoroughly opposed to this proposition on all grounds, the precedent it sets is far more horrifying than the idea itself. It is a move made out of desperation and fear, without any thought to the future it ushers in. Your online presence is and should be irrelevant, and should it become relevant, it will be dealt with then by the authorities already in place. Preemptive screenings of your social media information is a waste of money, a waste of time, and a breeding ground for hatred. DHS should not stoop so low as to fall to fear-mongering tactics to protect our country when all available information and studies point to the inefficacy of said tactics. Your life is not subject to the whims of a governing body.

-----

Comment Submitted by Maureen Rogers

Comment

View document:

There has to be a way without asking for the info. Anyone with a semblance of intelligence would lie on the form.

-----

Comment Submitted by Michael Lafferty

Comment

View document:

Social media accounts are private and should not be scanned by default or added to a government database.

-----

Comment Submitted by Christy [Last Name Unknown]

Comment

View document:

This seems like a massive waste of taxpayer money, particularly when it comes to screening US citizens re-entering the country. I can see the potential relevance if someone is on a no-fly list, or is flagged for suspicious behavior; however, screening every single person is a gratuitous waste of resources. Also, to be considered - it is incredibly easy to establish dummy accounts filled with inane information. Some of my friends have Facebook profiles for their pets, which they use exclusively to play Facebook games and send in-game resources back and forth with their main account. If it's that

easy to establish an account for a non-human entity like a pet, it seems to me that it would also be easy to establish a dummy account to make a person look harmless. Provide the details for the dummy account instead of your real one, and hey! You look like a different person. So this invasion of privacy for law-abiding citizens will still do nothing to hinder those looking to evade the law.

---

Comment Submitted by Nicholas Weaver

Comment

[View document:](#)

Public data is public: There have already been cases of other countries acting on social network data. If your persona online is public it is a decent source for data.

---

Comment Submitted by Jen Matheson

Comment

[View document:](#)

I am a Canadian and I am extremely against the collection and retention of my data by any country, including my own. I would not, under any circumstances travel to the U.S. if they were asking for my private information and social media accounts.

---

Comment Submitted by Svetlozar Mladenov

Comment

[View document:](#)

I can see the point of DHS, but let's face it: people who shouldn't be in the US probably already are. The recent attacks in France are still in the news. The people that conducted these attacks were *\*born\** in there. Most of the people travelling on an every day basis are *\*not\** terrorists, crooks, villains. Besides, even if the turnover of social media accounts is mandatory, a person can always have more than one account. And can always give-in the safe one. What about that scenario?

A lot of money from taxpayers, a lot of time lost at airports, a lot of aggravated travellers. A lot of tension building up.

---

Comment Submitted by David Seagrave

Comment

[View document:](#)

Will not be visiting now or in the future.

---

Comment Submitted by Angela Penrose

Comment

View document:

Spending \$300,000,000 to collect social media info, when people with something to hide on social media will just lie about not having accounts, or will only turn in the user names of their MomSafe accounts, is stupid. If DHS has an actual reason to investigate someone, they can use Google to find that person's social media like everyone else. Scanning social media on everyone who comes into the country is a ridiculous and useless waste of money and other resources, especially when it'd be trivially easy for a guilty person to hide/withhold the info.

---

Comment Submitted by Jim Sander

Comment

View document:

Hah, they don't represent the American my Grandfather fought to defend.

---

Comment Submitted by Jim Swanson

Comment

View document:

We have become a fascist state, with war-mongering, money grubbing tools of the plutocracy running the show. We need a left wing revolution NOW> Obomber, W, Dick, Donald, Hillary and Bill all belong in maximum security cells for life under no human contact restrictions. I have twice been sentenced to Federal prisons for political beliefs and know that they will be monitoring this form.

---

Comment Submitted by Lisa Krueger

Comment

View document:

No thank you. Un American.

---

Comment Submitted by Charles Lowe



Comment

[View document:](#)

Back off. These are recreational platforms. Those sites which indicate a significant security risk are already discernable. And Big Brother (e. g. NSA, GCHQ - UK) has proven that mass data collection does not remove their impotence, it just fuels our rebellion against Big Brother.

---

Comment Submitted by Andre Martin

Comment

[View document:](#)

Let's follow our ideals. Freedom of speech without chilling it by mass surveillance. If you have reason to believe someone is a threat then get a warrant or deny the travel visa prior to reaching the border. Don't subject the entire population to something to try and catch the outlier when you already have other tools available.

---

Comment Submitted by Richard Kosinski

Comment

[View document:](#)

No good.

---

Comment Submitted by Gervase Markham

Comment

[View document:](#)

If the DHS depends on voluntary disclosure of social media information to determine who is a risk to the United States, one might think they are not very good at their job. The bad guys will just lie, and the good guys will get caught in the inevitable hassle of false positives. It's as terrible an idea as the question asking people are you or were you ever a Nazi? - please ditch it.

---

Comment Submitted by Evan Thompson

Comment

[View document:](#)

This would be cause enough for me to renounce my citizenship and move to another country. Of course, I'd continue to work for US companies and buy Chinese products so... well you figure out the benefit to US GOVT.

---

Comment Submitted by Dave Turner

Comment

View document:

If you monitor Social Media in this way you will suppress the sharing of ideas. It is the sharing of thoughts and new ideas that has made human societies more aware and more civilised and delivers much more good than it does evil. You may think you are doing good but the direct obvious path is rarely the right path. Think more deeply about what you are doing. Leave people to be free online.

---

Comment Submitted by Myriam Thyres

Comment

View document:

This is absolutely inadmissible. No government or security agency should have access to our private lives without cause for suspicion.

---

Comment Submitted by James Penrose

Comment

View document:

It is invasive and unconstitutional on the face of it. For people in secondary, some scrutiny is allowable. Searches should be limited to personal items and any other materials being carried across the border only.

---

Comment Submitted by Sarah McKee

Comment

View document:

I am a former federal prosecutor and former General Counsel of the Interpol U.S. National Central Bureau in Washington, D.C. These proposals would violate the 4th Amendment to the U.S. Constitution. Entering the country or having entered the country does not constitute probable cause to believe that a crime has been committed, so as to provide the basis for a judicially-issued search warrant for a traveler's social media records. This would also clear the way for wholesale violation of

the rights to free speech and association. This would include the 1st and 4th amendment rights of persons in communication with an traveler who arrives or has arrived in the U.S. The proposal is unworthy of those who have taken an oath to protect and defend the U.S. Constitution against all enemies, foreign and domestic. Please withdraw it at once.

---

Comment Submitted by David Roberts

Comment

[View document:](#)

Demonstrates that governments no more trust us than we do them.

---

Comment Submitted by M.E. Stewart

Comment

[View document:](#)

I think it's a terrible idea. It's invasive, ill-advised, and unlikely to be at all useful. Someone planning to cause trouble will just make a skeleton account with whatever information they want.

---

Comment Submitted by Chris Marsh

Comment

[View document:](#)

It is none of your business, This is the UNITED STATES OF AMERICA not RUSSIA or the USSR

---

Comment Submitted by Emilia Tragon

Comment

[View document:](#)

I believe it is a very good idea. There's often outrage on why people weren't caught sooner when their facebook, twitter etc often display hints of sympathy towards terrorists (or white supremacists or other hate groups). Now the government will have access to those and can assess threats better. If we want transparency from the government, then we should also be transparent. Otherwise we're being hypocritical.

---

Comment Submitted by Richard Stallman

Comment

[View document:](#)

In general, your protect us from small dangers at tremendous cost to our freedom.

---

Comment Submitted by Soleil Lapierre

Comment

[View document:](#)

Gross and unjustifiable invasion of privacy.

---

Comment Submitted by Stu Maclean

Comment

[View document:](#)

You do not have my permission to access anything of mine. Kindly bugger off and mind your own business. Do you want to destroy your own tourism industry?

---

Comment Submitted by Anastasia Kaufmann

Comment

[View document:](#)

I strongly oppose it. I think it's invasive, unlikely to provide significant benefits, and will have a huge cost associated with it.

---

Comment Submitted by John West

Comment

[View document:](#)

I have no problem with many of the questions I answered no to if the government has a court order to do so but if not the government should not have open access to a person's social media accounts. I have no social media accounts other than regular email and the idea that I might be treated with more suspicion at the border because of this is abhorrent. I realize the reality of the need to increase border security in the world we live in today but this is a very flawed and ineffective way to do it as well as being very cost inefficient.

---

Comment Submitted by Lesley Schultz

Comment

View document:

This program would do nothing to stop terrorism. The US should stop these ruinous illegal and pointless wars abroad and start treating people with dignity and compassion at home. That would help a lot.

---

Comment Submitted by Ty Myrick

Comment

View document:

How this no a First and Fourth Amendment violation of free speech, free assembly, and security in our papers and effects.

---

Comment Submitted by Vincent Silenzio

Comment

View document:

As Benjamin Franklin has said, 'Those who surrender freedom for security will not have, nor do they deserve, either one.' Mass surveillance and policing that would dampen or restrict any person's freedom of expression is not only un-American, it is counterproductive.

---

Comment Submitted by Martin Washington

Comment

View document:

NONE OF HOMELAND SECURITY BUISNESS!

---

Comment Submitted by Treva Lewis

Comment

View document:

This is a grievous breach of privacy in line with doxxers and black hat hackers, not fitting for the government to be involved in. In addition, I highly doubt that reading someone's personal Facebook

feed would provide any useful information for US security; practically speaking, it would be a huge waste of money and resources.

---

Comment Submitted by Eldon Rosenberg

Comment

View document:

If you want to win the war on terror, the first step is to stop acting like you've already lost it (living in fear).

---

Comment Submitted by Noel da Costa

Comment

View document:

It doesn't make sense to ask for social media handles.. these can be changed at any time by just opening a new social media account... so it won't stop criminals. All it does is compromise the privacy of random people. Not cool.

---

Comment Submitted by Patrick Vingo

Comment

View document:

Being presumed possibly guilty of wrong doing by having your social media checked on entering the country is an invasion of privacy. The only justification for doing so is if someone is detained by customs because a real red flag has been raised or a person is on a known watch list for suspected criminal activity.

---

Comment Submitted by Lana Melnichuk

Comment

View document:

They are welcome to search my name on Google and discover all publicly available data. Anything under password/privacy is not for government to see.

---

Comment Submitted by Alison Johnson

Comment

[View document:](#)

My freedom is more important to me than the idea of absolute safety. I also know that no government, not even the Big Brother government that Orwell envisioned, can provide absolute safety, or even substantially improved safety. The proposed plan is dangerously un-American: targeting people based on the statements of an acquaintance of an acquaintance, targeting people based on statements that those currently in power don't like. I want to be free to describe Donald Trump as Cheeto Jesus, a baby-fingered shitgibbon, or a merkin-headed man-baby without fear of being hauled in for questioning by his secret police. Also, fuck you for even thinking this plan is a good idea.

---

Comment Submitted by Janelle Witter

Comment

[View document:](#)

This is a gross infringement of my privacy.

---

Comment Submitted by O O

Comment

[View document:](#)

UnAmerican! Without probable cause, it's not the government's business to spy upon citizens.

---

Comment Submitted by Glenn McAnally

Comment

[View document:](#)

This is clearly unreasonable search and seizure. It is irrelevant whether the person being violated in this way is a U.S. citizen or not.

---

Comment Submitted by Luis Lozano

Comment

[View document:](#)

If they really want to know what my cat did this morning they can get a warrant.

---

Comment Submitted by Russell Neches

Comment

View document:

The only justifiable reason to conduct such a search is if there is already probable cause to suspect a violation or planned violation of the relevant US laws. For example, if Customs agents suspected that a person might be attempting to enter the United States under an assumed identity, it would be reasonable to compare the documents submitted to the relevant social media accounts (for example, to make sure the names and photographs all appear to belong to the same person). If there were probable cause to suspect that someone was seeking entry into the United States with the intention of harming another person -- an ex-girlfriend, for example -- it would be reasonable to examine the traveler's social media posts to see if they contained menacing language.

It would not be reasonable, nor ethical, nor lawful, to examine someone's social media presence without probable cause, or having done so, to take action based on speech that is protected by the Constitution. For example, suppose a search is conducted because there was reason to suspect the traveler of seeking entry under an assumed identity; speech of a political nature must to be considered irrelevant.

Moreover, if a search conducted on the basis of probable cause yielded speech of a questionable nature -- say, a selfie of the person in question smoking pot -- it should not be deemed pertinent to the person's intent regarding their behavior while in the United States.

Any policy for examining social media should be based on the principle that information gleaned from social media is of suspect veracity. It should be ASSUMED that there is likely to be deliberate manipulation, both favorable and unfavorable, of that person's presentation on social media. It must be TAKEN AS A GIVEN that the subject manipulates their own presentation (as is their right), but also that third parties may also manipulate their presentation. Third parties may have malicious intent towards the subject, or towards the Unite...

---

Comment Submitted by Rick Potthoff

Comment

View document:

It's unAmerican, unconstitutional & counterproductive (if you're searsching for a needle in a haystack, why make the haystack bigger?)

---

Comment Submitted by Amanda Jacobs

Comment



[View document:](#)

Deeply intrusive. Echoes of the thought police and George Orwell's 1984

---

Comment Submitted by Teddy Woodhouse

Comment

[View document:](#)

Besides the Big Brother vibes that come from this proposal, the price tag for this program alone should give pause. There are better anti-terrorism tactics that can be pursued rather than building a social media monitoring megatron and requiring individuals to submit this personal information to be stored on databases, after the series of leaks of PII from the federal government. This idea, while well intentioned, is riddled with problems and holds little evidence of being effective.

---

Comment Submitted by Andrew Roach

Comment

[View document:](#)

I think this plan is ridiculous, Orwellian, and overbearing.

---

Comment Submitted by Bence Kormos

Comment

[View document:](#)

It's ridiculous! I am fairly sure that all unwanted entities use a different - possibly private - channel to spread their unwanted things. This completely paranoid and it's just a waste of all kinds of resources while completely breaching basic online privacy and the right to keep your information private!

---

Comment Submitted by Lyndsay Saunders

Comment

[View document:](#)

I feel the proposed action is a violation of my right to privacy.

---

Comment Submitted by Michael Ketchen

Comment

[View document:](#)

Without a warrant or probable cause, this is a violation of the Fourth Amendment.

---

Comment Submitted by Peter Lentjes

Comment

[View document:](#)

Please stop taking away the freedom of people step by step. Big Brother is peeping at us far too much already.

---

Comment Submitted by Frann Leach

Comment

[View document:](#)

If I was a US tax payer I'd tell them it was a waste of time and money.

---

Comment Submitted by James Stephenson

Comment

[View document:](#)

NO WAY, no probable cause exists

---

Comment Submitted by Tandy Sturgeon

Comment

[View document:](#)

For individuals who have no criminal record, this is quite simply an unlawful invasion of privacy.

---

Comment Submitted by Thomas Pauley

Comment

[View document:](#)

No-Never!

---

Comment Submitted by Dave Knight

Comment

View document:

I think this is needless intrusion into people's lives when in the vulnerable position at a border and I don't think it's justified. You already have to give your fingerprints and a criminal check for a US visa, surely that is enough.

---

Comment Submitted by Asd Asd

Comment

View document:

No, respect privacy.

---

Comment Submitted by Garrett Murphy

Comment

View document:

Not a very good or remotely admirable idea at all!

---

Comment Submitted by Omer Katz

Comment

View document:

I understand the reasoning behind doing so as often ISIS, Al-Nusra and other terrorist organizations supporters declare their allegiance on social media but they may or may not be a threat. There is a genuine privacy-security tension here and that's why I'm not 100% sure the process has to be mandatory.

Retaining data of people not suspected of any wrongdoing is wrong. It won't assist the US to keep their borders safe anyway.

Denying entry on other grounds (such as political opinion or sexual orientation) other than the assested threat level is not what I'd expect from a democracy and will either censor people

interested to visit the US or prevent them from wanting to travel to the US. Any such incident should be dealt with as soon as possible to ensure due process.

---

Comment Submitted by Ari [Last Name Unknown]

Comment

[View document:](#)

For a country whose citizens are so rabidly opposed to government overreach this is a baffling direction in which to consider moving. Social media accounts may often fall under the no expectation of privacy rule, but considering what's said on them as a basis for allowing or banning entry to another country is tantamount to following someone around with a microphone and entering everything they say outside of their own house or a bathroom stall as grounds for limiting their passage across international borders. Not illegal, but definitely not something anyone sane would consider an acceptable degree of scrutiny.

It also opens the door to criminalizing free speech, which is another thing Americans are usually pretty fond of. I'm okay with potential criminal convictions being held against me - those are entered in the record as a breach of democratically-established laws - but you seriously can't be considering denying a person entry based on them saying something vaguely shady in a Tweet?? Not sure how this can be justifiable, given that the U.S.A. doesn't even have, say, real hate speech laws - and in Canada, if I'd been caught saying something illegal, it would already be in an official record somewhere as a criminal act, rendering the need for my social media usernames completely unnecessary.

A border control booth is not a court of law, and its occupants should not be encouraged to act like one.

---

Comment Submitted by Malcolm Tattersall

Comment

[View document:](#)

Enormously intrusive and with minuscule likely benefits.

---

Comment Submitted by Bryne Rasmussen

Comment

[View document:](#)

This is outrageous and will only create more paranoia and fear while stifling healthy dissent and not keep us any safer but create more violence.

---

Comment Submitted by Margaret Taylor-Bey

Comment

View document:

This is just another form of slavery, human control, and discrimination of the human race around the world that don't look like them

---

Comment Submitted by Janna Ostoya

Comment

View document:

Searching a person's online presence represents a gross invasion of privacy and a departure from the ideals set forth in the Bill of Rights.

---

Comment Submitted by Thomas Russ

Comment

View document:

The 4th amendment to the Constitution should govern government searches, so searches of online presence should only be made pursuant to a valid search warrant or court order. These must be presented to the subject of the search.

---

Comment Submitted by Julie White

Comment

View document:

Awful and invasive

---

Comment Submitted by I I

Comment

View document:

Stupid idea. It's none of your business and you're already invading everyone's privacy way too much! Besides, adding more hay to the haystack won't help you find the needle.

---

Comment Submitted by J.T. Smith

Comment

View document:

I think this plan is a complete invasion of privacy and should be considered a human rights violation. Trying to claim that it's somehow meant to deter or help locate terrorists only demonstrates that: 1) you have no grasp of reality as the lone wolf terrorists that you fear the most are least likely to discuss their plans with anyone else; and two 2) you fail to realize that trying to go to war on terrorism proves that A you're afraid which means that you have already lost the war because the ENTIRE purpose of terrorism, regardless of political clothes it wears, is to instill terror, and B you fail to realize that by trying to physically fight terrorism or use ANY terroristic tactics (like forcibly invading people's privacy) only serves to create more of the very enemies you're trying to fight!

---

Comment Submitted by Fredrick McDonald

Comment

View document:

Another pointless program that does nothing to keep our citizens safe. No, thank you.

---

Comment Submitted by Jeff Lyon

Comment

View document:

This a stupid idea, waste of taxpayer money, and won't keep us secure. You already have more data than you know what to do with, much of it gathered unconstitutionally. You couldn't stop the Orlando attacks or the Boston Marathon bombing despite having incriminating data on the perpetrators. Your authoritarian tactics and waste of taxpayer resources on defense industry contracts is shameful, and you should be ashamed.

---

Comment Submitted by Janice Urbsaitis

Comment

View document:

I think this is intrusive and can be used against each citizen and that maybe social media as a construct was designed with this ultimate purpose in mind. There is no real privacy anywhere anymore.

-----

**Comments on the Customs and Border Protection Bureau (USCBP) Notice: [Agency Information Collection Activities: Arrival and Departure Record \(Forms I-94 and I-94W\) and Electronic System for Travel Authorization](#)**

Page 6

Comment Submitted by Danielle McManus

Comment

View document:

The proposal is invasive and its use a profound abuse of power. To invade people's social media accounts--particularly without their consent--is an incredible miscarriage of justice.

---

Comment Submitted by Peter Kjeldsen

Comment

The fact is that I don't have any social media accounts. I have no interest in social media, I am aware of all of the social media variants, but I never felt they offered me anything and I don't think it is fair that I should be singled out for special attention, just because I don't feel the need to be part of an artificial community of mostly imbeciles.

*No documents available.*

Attachments

View All (0)

---

Comment Submitted by Jose Magana- Salgado, Immigrant Legal Resource Center

---

Comment



<b>Hon. Nancy Pelosi</b>	<b>Bill Ong Hing</b>
<b>Hon. Cruz Reynoso</b>	90 K Street NE., 10th Floor
Board of Directors	Of Counsel
<b>Cynthia Alvarez</b>	<b>Don Ungar</b>
<b>Richard Boswell</b>	Washington, DC 20229-1177
<b>W. Hardy Callcott</b>	Executive Director
<b>Eva Grove</b>	<b>Eric Cohen</b>
<b>Bill Ong Hing</b>	<b>RE: Agency Information Collection Activities: Arrival and Departure Record (Forms I–94 and I–94W) and Electronic System for Travel Authorization; (June 23, 2016); Docket No. 2016-14848; OMB Control Number 1651-0111.</b>
<b>Lisa P. Lindelef</b>	
<b>Anita I. Martinez</b>	San Francisco
<b>Michelle Mercer</b>	1663 Mission Street
<b>Toni Rembe</b>	Suite 602
<b>Rudy Ruano</b>	San Francisco, CA 94103
August 22, 2016	t: 415.255.9499
<b>Guadalupe Siordia-Ortiz</b>	f: 415.255.9792
Paperwork	Washington D.C.
Reduction Act	1016 16th Street, NW
Officer	Suite 100
<b>Lisa Spiegel</b>	Washington, DC 20036
<b>Reginald D. Steer</b>	t: 202.777.8999
U.S. Customs and	f: 202.293.2849
Border Protection	
<b>Alan Tafapolsky</b>	Dear Paperwork Reduction Act Officer:
<b>Mawuena Tendar</b>	ilrc@ilrc.org
U.S. Department of	www.ilrc.org
Homeland Security	The Immigrant Legal Resource Center (ILRC) and the National Immigration Project of the National Lawyers Guild (NIPNLG) submit the following comment in response to Agency Information Collection Activities: Arrival and Departure Record (Forms I–94 and I–94W) and Electronic System for Travel Authorization. We write to oppose the collection of information associated with an individual's online presence—including social media websites, apps, and identifiers—by U.S. Customs and Border Protection (CBP) through Form I-94W, the Electronic System for Travel Authorization (ESTA), and all future information collections.
<b>Hon. James L. Warren (Ret.)</b>	
<b>Allen S. Weiner</b>	
Regulations and	
Rulings	
<b>Roger Wu</b>	Founded in 1979, ILRC is a national resource center that provides training, consultations, publications, and advocacy support to individuals and groups assisting low-income persons with immigration matters. ILRC works with a broad array of individuals, agencies, and institutions, including immigration attorneys and advocates, criminal defense
General Counsel	
Office of Trade	

attorneys, civil rights advocates, social workers, law enforcement, judges, and local and state elected officials. ILRC is uniquely qualified to provide comments regarding the proposed rulemaking in light of its extensive training of practitioners regarding admissibility and related issues. This extensive technical knowledge includes regular trainings, seminars, and advisories, including *Inadmissibility & Deportability*,<sup>1</sup> *Contesting Removal*,<sup>2</sup>

<sup>1</sup> ILRC Staff Attorneys, INADMISSIBILITY & DEPORTABILITY, (Immigrant Legal Resource Center) (3rd ed. 2013).

<sup>2</sup> Contesting Removal, *Trainings & Seminars*, IMMIGRANT LEGAL RESOURCE CENTER (Last accessed July 19, 2016), <http://www.ilrc.org/trainings-webinars/recorded-webinars/contesting-removal>. *Comment on CBP Collection of Social Media Identifiers* [Docket No. USCIS-2016-

*LGBTQ Immigration: Ensuring Quality for All*,<sup>3</sup> and other guidance. In light of this deep reservoir of technical knowledge, we submit the below comment.

3 Lourdes Martinez, *LGBTQ IMMIGRATION: ENSURING EQUALITY FOR ALL*, (Immigrant Legal Resource Center) (1st ed. 2015).

4 Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization, 81 Fed. Reg. 40892, 40892 (June 23, 2016), *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>.

5 Andrew Perrin, *Social Media Usage: 2005-2015*, PEW RESEARCH CENTER, Oct. 8, 2015, <http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/>.

6 Id.

NIPNLG is a national non-profit that provides legal and technical support to legal practitioners, immigrant communities, and advocates seeking to advance the rights of noncitizens. For over forty years, NIPNLG has been promoting justice and equality of treatment in all areas of immigration law, the criminal justice system, and social policies related to immigration. The organization's success is built upon a national membership that includes attorneys, law students, judges, jailhouse lawyers, advocates, community organizations, and other individuals seeking to defend and expand the rights of immigrants in the United States.

## INTRODUCTION

CBP proposes to incorporate the following questions to Form I-94W and ESTA "Please enter information associated with your online presence—Provider/Platform—Social media identifier."<sup>4</sup> ILRC and NIPNLG express our vehement opposition to the incorporation of this information collection and strongly opposes any proposed information collection that seeks to obtain the social media identifiers and accounts of individuals seeking entry or admission. Nearly 65% of adults employ one or more social media websites, representing a dramatic increase from the last decade.<sup>5</sup> Individuals use social media to discuss and share information related to employment, politics, communications, health, civic life, consumption of news, local communities, parenting, dating, and more.<sup>6</sup> Consequently, social media presents a detailed mosaic of an individual's private and personal life, personal preferences, and intimate associations.

Many individuals coming to the U.S. are fleeing oppressive regimes that monitor, limit, and restrict the usage of social media. In many cases, foreign governments monitor social media to identify political opponents and restrict access to social media to make peaceful protests and government opposition more difficult. Requesting that individuals arriving to the U.S. provide social media information risks perpetuating the governmental systems that foster the very persecution and oppression that caused these individuals to flee in the first place.

This information should not be collected because it is not reliable and, in the cases of immigration screenings, inappropriate use of social media to determine an individual's admissibility or assess an individual's national security profile. Aside from the logistical, due process, and procedural concerns with the collection of this data, this information collection represents a dangerous precedent and

As detailed below, information collection revolving around social media presents significant technical and privacy considerations that makes it inappropriate for the purposes of immigration screening:

**❑❑CBP's proposed collection is vague, overbroad, and threatens political speech.** People use social media to express political ideas and share critical analyses of society and government. Through geotagged photos and videos, CBP is essentially requesting information that would map out an individual's entire history of movement, activities, associations, and ideas. Moreover, the collection of immigrants' personal online identifiers—which can intersect financial, dating, and political websites—to track these activities risks encroaching on civic and political participation and chilling the exercise of rights protected under the First Amendment.

**❑❑Collection of social media information will likely lead to the collection of stale and inaccurate information that would unduly prejudice individuals.** Underlying the very nature of social media is the ability of third parties to associate an individual with specific content *without* the consent of the individual. Ultimately, CBP should employ more trustworthy investigative methods to assess an individual's background, including in-person interviews and use of reliable records to accurately and efficiently assess admissibility and national security concerns.

**❑❑It is very unclear how truly optional this collection will be.** CBP fails to state exactly how it would communicate to individuals that the information collection would represent an “optional data field.” Without an explicit statement regarding the optional nature of the field, individuals will likely and reasonably presume that the information is required. Yet it is entirely unclear how the information will be used, and how inappropriate use of the information could be monitored or remedied.

**❑❑CBP grossly underestimates the information collection burden upon individuals.** CBP does not consider that the average individual likely has a multitude of social media identifiers, each of which carries an associated burden of disclosure. For example, an individual may have to carefully catalogue every single social media network—or network that could arguably be considered social media—for disclosure. CBP currently estimates time per response at 16 minutes for the entirety of Form I-94W and at 23 minutes for ESTA, far too little time for an individual to accurately include all social media identifiers.

## 1. PROPOSED INFORMATION COLLECTION IMPERMISSIBLY THREATENS POLITICAL PARTICIPATION

Through the proposed information collection, CBP is impermissibly asking individuals to reveal a wealth of information regarding an individual's participation in political and civic engagement activities.<sup>7</sup> Indeed, 66% of all social media users engaged certain civic or political activities

<sup>7</sup> See *Talley v. California*, 362 U.S. 60, 64-65 (1960) (holding that the government cannot compel individuals to identify themselves on speech they distribute); *Thornburgh v. American College of*

*Obstetricians & Gynecologists*, 476 U.S. 747, 767 (1986) (“[T]he Court consistently has refused to allow government to chill the exercise of *Comment on CBP Collection of Social Media Identifiers* [Docket No. USCIS-2016-14848; OMB Control Number 1615-0111. Page 4 of 10

4

constitutional rights by requiring disclosure of protected, but sometimes unpopular, activities.”); *NAACP v. Alabama*, 357 U.S. 449, 461 (1958).

8 *Politics Fact Sheet*, PEW RESEARCH CENTER, Nov. 14, 2012, <http://www.pewinternet.org/fact-sheets/politics-fact-sheet/>.

9 *National Border Patrol Council Endorses Donald Trump for President*, National Border Patrol Council, March 30, 2016, <http://www.bpunion.org/index.php/newsroom/press-releases/1824-national-border-patrol-council-endorses-donald-trump-for-president>.

10 HRW: Research on Customs and Border Protection Abuses Facebook Page, Human Rights Watch, (last accessed August 12, 2016), <https://www.facebook.com/HRWborderrights/>.

11 357 U.S. 449, 461 (1958).

through social media, supporting political or social issues originally shared by a third party (38%), shared their own opinions on political and social issues (34%), encouraged others to act on a political or social issue (31%), belonged to an online group dedicated to a political or social issue (21%), or follow candidates for political office (20%).<sup>8</sup> By requesting an individual’s social media information, CBP is not only asking for their online presence, but an entire annotated history that individual’s political leanings on social and political issues. Such a request for information lends itself to potential abuse and harassment by CBP officers who disagree with an individual’s political leanings, particularly in light of the unprecedented endorsement of Republican Nominee for President, Donald Trump by the National Border Patrol Council, which represents 16,500 border patrol agents.<sup>9</sup>

Moreover, individuals who participate in organizations and actions geared toward CBP accountability or immigrant rights may find themselves targeted after revealing this information, as CBP officers will likely not look positively on individuals who have a demonstrated history of advocating for accountability for CBP. Nor is this concern hypothetical, an individual with Facebook who is part of “Human Rights Watch: Research on Customs and Border Protection Abuses”<sup>10</sup> or who follows @Not1\_More on Twitter—which advocates for the end of all deportations—could quickly find herself in the crosshairs of a CBP agent who disagrees with her advocacy. In particular, individuals who come to the U.S. and stay near the border may have significant contact with CBP even outside of Ports of Entry.

Consequently, the proposed information collection raises serious concerns regarding chilling freedom of speech. As previously stated, social media is regularly used for civic participation in political and social issues. However, if CBP demands that information regarding these types of activities is disclosed, individuals would be less likely to openly participate in these activities. There is little doubt that an individual engaged in advocacy around accountability for CBP, immigration, or civil liberties issues would think twice about publically speaking on these issues on social media accounts that they knew would be monitored by CBP. Indeed, as the Supreme Court noted in *NAACP v. Alabama*, even when chilling of

speech occurs unintentionally as a result of government action, violation of the First Amendment can still occur.<sup>11</sup> In *NAACP*, the primary issue was the compelled disclosure of an organization's membership list, striking a similar parallel to CBP's proposed information collection of social media identifiers, which often link a series of likeminded individuals through a discrete, identifiable member group. *Comment on CBP Collection of Social Media Identifiers* [Docket No. USCIS-2016-14848; OMB Control Number 1615-0111. Page 5 of 10

5

## **2. PROPOSED INFORMATION COLLECTION IS TREMENDOUSLY OVERBROAD, COLLATERAL, AND UNNECESSARY**

As a result of the nature of social media, the proposed information collection will inadvertently lead to the disclosure of a tremendous amount of collateral and unnecessary information that may facilitate discrimination, profiling, and unneeded investigation. As stated above, social media intersects with virtually every aspect of an individual's life, including friends, family, religion, shopping, dating, civic engagement, and more. Consequently, this information request is not only asking individuals to disclose their social media identifiers, but all of the sensitive, personal, and intimate information associated with those identifiers. There would be little argument that an information collection centering around an individual's religion, sexual orientation, political opinions, purchase history, or list of friends would be grossly overbroad and inappropriate. And yet, CBP would ask an individual to provide this information through the disclosure of social media identifiers. CBP should not make an overbroad request for intimate and personal information that is unreliable for any legitimate agency purposes. This information collection, at best, is an overbroad fishing expedition that will function as a dragnet for a variety of sensitive and personal information.

Membership in certain social media networks reveals a panoply of sensitive information. For example, 27% of 18- to 24- year olds use online dating, with one-in-five employing mobile dating apps.<sup>12</sup> Dating social media websites present a unique danger in the over disclosure of sensitive information, with many dating social media websites being targeted to specific demographics, such as Chemistry.com (for LGBT individuals), Christian Mingle (for Christian individuals), JDate (for Jewish individuals), and more. Essentially, membership in these social media websites would disclose an innate and intimate piece of personal information to CBP officers reviewing an individual's social media identifiers, such as sexual orientation or religion.

12 Aaron Smith and Monica Anderson, *5 facts about online dating*, PEW RESEARCH CENTER, Feb. 29, 2016, <http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/>.

13 Michal Kosinski, et. al, Private traits and attributes are predictable from digital records of human behavior, *PROCEEDINGS OF THE NATIONAL ACADEMY OF SCIENCES OF THE UNITED STATES OF AMERICA*, April 9, 2013, <http://www.pnas.org/content/110/15/5802.abstract>; Raphael Satter, *Facebook Privacy: 'Liking' A Page Can Reveal Intimate Details About You*, ASSOCIATED PRESS, May 11, 2013, [http://www.huffingtonpost.ca/2013/03/11/facebook-privacy-like-button\\_n\\_2854556.html](http://www.huffingtonpost.ca/2013/03/11/facebook-privacy-like-button_n_2854556.html).

Similarly, membership in Facebook "groups" (which allow individuals to join together around a particular topic or issue) or liking of certain "pages" (which allow individuals to express support of a

particular topic, issue, or person) would quickly disclose intimate details about an individual's life. For example, the Proceedings of the National Academy of Sciences analyzed more than 58,000 Facebook profiles and found that they could directly link an individual's "Likes" to "sexual orientation, gender, age, ethnicity, IQ, religion, [and] politics . . . . The likes also mapped to relationship status, number of Facebook friends, as well as half a dozen different personality traits."<sup>13</sup> Ultimately, the overwhelming majority of this information is collateral and unrelated to the processes involved in determining whether an individual is inadmissible and this excess of information is likely ripe for abuse, profiling, or extraneous questions or investigation. *Comment on CBP Collection of Social Media Identifiers [Docket No. USCIS-2016-14848; OMB Control Number 1615-0111. Page 6 of 10*

6

### 3. PROPOSED COLLECTION WILL COLLECT STALE AND INACCURATE INFORMATION

Collection of social media information presents unique obstacles regarding veracity and accuracy of the information. Specifically, underlying the very nature of social media is the ability of third parties to associate an individual with specific content *without* the consent of the individual. For example, Facebook allows third-party individuals to post content—such as links, written content, photos, and videos—to an individual's timeline<sup>14</sup> (e.g. an individual's public-facing Facebook page) or even "tag" an individual in a photo or video.<sup>15</sup> Facebook also allows you to "tag" other people that you are with, essentially allowing individuals to claim that they were physically with another individual.<sup>16</sup> Twitter allows third-party individuals to "follow" an individual's Twitter account<sup>17</sup> and tweet at an individual by referencing an individual's twitter "handle" in a tweet.<sup>18</sup> Like Facebook, Instagram allows individuals to "tag" individuals in photos and videos.<sup>19</sup> Practically, this means that an individual's social media account can be associated with inaccurate and potentially problematic information by third parties.

14 *How do I post something on someone else's timeline?*, Facebook Help Center (last accessed Aug. 12, 2016), <https://www.facebook.com/help/173433019380025>.

15 *How do I tag myself or my friends in photos?*, Facebook Help Center (last accessed Aug. 12, 2016), <https://www.facebook.com/help/227499947267037>.

16 *How do I post something on someone else's timeline?*, Facebook Help Center (last accessed Aug. 12, 2016), <https://www.facebook.com/help/173433019380025>.

17 *Following people on Twitter*, Twitter Help Center (last accessed Aug. 12, 2016), <https://support.twitter.com/articles/162981>.

18 *Types of Tweets and where they appear*, Twitter Help Center (last accessed Aug. 12, 2016), <https://support.twitter.com/articles/119138>.

19 *How do I tag people in my photo?*, Instagram (last accessed Aug. 12, 2016), <https://help.instagram.com/174635396025538>.

For example, shortly before CBP's review of an individual's social media profile, a third-party individual could "tag" and falsely associate an individual potential grounds of inadmissibility or national security concerns. As another example, on Facebook, a friend could "tag" an individual in a photo of drugs

(leading to further investigation regarding drug-related inadmissibility), alcohol (triggering concerns related to habitual drunkard inadmissibility concerns), or gang paraphernalia or symbols (triggering public safety concerns). On Twitter, accounts associated with terrorism or terrorist groups could, without limitation, follow and tweet at an individual. On Instagram, an individual could tag an individual in a photo that contains guns or other prohibited weapons. In all of these examples, an individual would have little to no control as to whether these tags and associations appear on their social media networks, even if they are completely erroneous. Investigators would be overwhelmed with unproductive and inaccurate leads while innocent parties would have their backgrounds scrutinized for no legitimate reason.

Collection of information from social media networks is inherently problematic, erroneous, and unreliable because of the ability of third-parties to *unilaterally* associate an individual with potentially inaccurate content. CBP will be inundated with substantial and questionable information—much of it provided by third parties—that will exhaust its investigative capabilities and erroneously elevate innocent individuals for closer scrutiny. Ultimately, CBP should and can turn to more trustworthy investigative methods to assess an individual’s *Comment on CBP Collection of Social Media Identifiers* [Docket No. USCIS-2016-14848; OMB Control Number 1615-0111. Page 7 of 10

7

background, including in-person interviews and use of reliable records to accurately and efficiently assess admissibility and national security concerns.

#### **4. PROPOSED INFORMATION COLLECTION IS VAGUE**

Social media is defined as a form of “electronic communication . . . through which users create online communities to share information, ideas, personal messages, and other content.”<sup>20</sup> Consequently, this definition encompasses an enormous amount of different online services, from web sites considered traditional social media, such as Facebook; to image sharing sites, such as Flickr and Instagram; to financial transaction websites and apps, such as Venmo<sup>21</sup> and Amazon,<sup>22</sup> which allows users to share purchase and money transfer history with friends; to a variety of dating websites and apps. CBP requests that individuals provide information associated with their “[s]ocial media identifier” but fails to outline any sort of limiting factor regarding what type of information or social media CBP seeks. Consequently, an individual could reasonably believe that an individual must disclose excessive and extraneous information regarding their online process, everything from shopping, to dating, to photo sharing because of the vagueness of the information collections. Others could reasonably believe that social media is limited to certain networks, such as Facebook, one of the most commonly known and recognized social media networks.

<sup>20</sup> Merriam Webster Dictionary, Definition of “social media” (last accessed Aug. 12, 2016), <http://www.merriam-webster.com/dictionary/social%20media>.

<sup>21</sup> Aran Khanna, *Your Venmo Transactions Leave a Publicly Accessible Money Trail*, THE HUFFINGTON POST, Oct. 30, 2015, [http://www.huffingtonpost.com/aran-khanna/venmo-money\\_b\\_8418130.html](http://www.huffingtonpost.com/aran-khanna/venmo-money_b_8418130.html).



22 Matthew Humphries, *Amazon lets you buy and share on Facebook*, GEEK, Mar. 17, 2008, <http://www.geek.com/news/amazon-lets-you-buy-and-share-on-facebook-573431/>.

23 Geotagging Definition, TECHOPEDIA (last accessed Aug. 12, 2016), <https://www.techopedia.com/definition/86/geotagging>.

The lack of a specific definition of social media in the information collection will lead to a disparate set of responses from individuals, with some responses being under inclusive and others being over inclusive. In terms of social media, there is no limiting principle regarding what constitutes a “social media” website or app as a significant portion of websites and apps now have mechanisms to share content with friends. Consequently, there is no manner in which CBP could narrowly tailor this request or make it an appropriate screening question for individuals seeking admission.

## 5. PROPOSED INFORMATION COLLECTION INCLUDES DETAILED HISTORY OF MOVEMENT

By requesting social media identifiers for social media that allows individuals to upload and share photos and videos, CBP is asking for significantly more information than may be apparent. Specifically, social media—through geotagged photos and videos—has the potential to disclose an enormous amount of geographical and locational information to CBP, including a detailed map of the places, locations, and people that an individual visited.

Geotags are metadata that provide information regarding the physical location where a photo or video was taken, including latitude, longitude, altitude, distance, and name of a location.<sup>23</sup> Most GPS-enabled smartphones and cameras automatically incorporate geotags into photos *Comment on CBP Collection of Social Media Identifiers* [Docket No. USCIS-2016-14848; OMB Control Number 1615-0111. Page 8 of 10

8

and videos, raising significant privacy and safety concerns.<sup>24</sup> Disabling geotagging is often a cumbersome, unclear practice that most individuals do not engage in.<sup>25</sup> Consequently, geotagged photos and videos from social media sites, such as “Twitter, YouTube, Flickr, and Craigslist” can be “used to identify a person’s home and haunts.”<sup>26</sup> Thus, an individual that uploads a geotagged photo or video to a social media account disclosed to CBP risks sharing a tremendous amount of information that an individual may not have intended to share or disclose. This disclosure can include sensitive information, such as places where an individual worships, locations catering to individuals with certain sexual orientations, or visits to specialized medical facilities that would disclose private health issues. The fear of providing social media with links to photos with sensitive geo-tagged information is not speculative. Nearly *half* of young adults (18-29) who use the internet also use Instagram—a social media network that exclusively depends on the uploading and sharing of photos.<sup>27</sup>

24 Kate Murphy, *Web Photos That Reveal Secrets, Like Where You Live*, N.Y. TIMES, Aug. 11, 2016, <http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html>.

25 Id.

26 Id.

27 Maeve Duggan et. al, *Social Media Update 2014*, PEW RESEARCH CENTER, Jan. 9, 2015, <http://www.pewinternet.org/2015/01/09/social-media-update-2014/>; Taylor Hatmaker, *How to delete Instagram's secret map of where you live*, DAILY DOT, Feb. 20, 2015, <http://www.dailydot.com/debug/how-to-remove-instagram-geotags/>.

28 *Types of Tweets and where they appear*, Twitter Help Center (last accessed Aug. 12, 2016), <https://support.twitter.com/articles/119138>.

## **6. PROBLEMS WITH THE “OPTIONAL” NATURE OF PROPOSED INFORMATION COLLECTION**

The “optional” nature of the proposed information collection presents problems in the realm of misrepresentations and whether the information collection would be truly “optional.” First, CBP fails to state exactly how it would communicate to individuals that the information collection would represent an “optional data field.” Without an explicit statement to individuals regarding the optional nature of the field, individuals will likely, reasonably presume that the information is required. Even if the data field were billed as “optional,” it is extremely likely that individuals would feel pressured regarding the disclosure of the information, particularly in light of potential comments or harassment from CBP officers asking individuals why they chose not to provide the information. There is also a question of whether failing to provide this optional information would create a negative inference among CBP officers, with CBP officers singling out individuals for additional screening based on their refusal to provide this optional information, or possibly charges of inadmissibility based on misrepresentation. Finally, there is an open question as to how long such a field would remain optional and whether CBP would seek to make this field mandatory during future notice and comment periods.

## **7. LACK OF CLARITY IN USE AND DUE PROCESS REGARDING INFORMATION COLLECTION.**

CBP fails to outline exactly how the collected information will be used and shared by CBP. While CBP states that the information collection is in support of “its mission related to the screening of alien visitors for potential risks to national security and the determination of admissibility,”<sup>28</sup> it fails to outline how this information will be used. National security concerns often cut across multiple federal agencies and law enforcement authorities; consequently, there is an open *Comment on CBP Collection of Social Media Identifiers* [Docket No. USCIS-2016-14848; OMB Control Number 1615-0111. Page 9 of 10

9

question whether CBP will share the information it obtains with other agencies, such as U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, U.S. Department of Justice, FBI, NSA, and others. Additionally, CBP fails to outline how it will evaluate the information it finds online in regards to accuracy and reliability, particularly in situations where CBP is forwarding that information for interagency review.

In the context of basic due process and fairness, CBP does not outline how it will weigh the credibility of information found on social media networks—particularly when that information is shared onto an individual’s social network by a third party (as discussed above). There is no process in place for individuals to contest or dispute inaccurate or ambiguous information that may appear on an

individual's social media account. Moreover, the information collection presents an opportunity for CBP to use the collection information against an immigrant without proper advisals, explanation of how the information will be used, or a consultation with an attorney who could outline the pitfalls of voluntarily disclosing this sensitive information to CBP. Given that CBP provides a clear framework of how this information will be evaluated and shared and establishes processes in place to contest erroneous information, collection of this information is premature and inappropriate.

## **8. INFORMATION COLLECTION BURDEN IS HIGHER THAN CBP ESTIMATES**

CBP provides a variety of estimated time per response, with 16 minutes for the entirety of Form I-94W and 23 minutes for ESTA. These estimates, however, do not consider that the average individual likely has a multitude of social media identifiers and the burden likely associated with the disclosure of these identities. For example, an individual may have to carefully catalogue every single social media network—or network that could arguably be considered social media—for disclosure, lest they be charged with misrepresentation. Moreover, an individual would likely have to revisit social networks where they are members but whose accounts may have fallen into disuse in order to obtain and verify older credentials and social media identifiers. Individuals who want to verify exactly what *type* of information they are disclosing to CBP would also have to conduct a careful, individualized review of each social media account to determine what information is publically available and whether they are comfortable sharing that information with the federal government. Finally, individuals who want to limit the amount of public information they share with CBP, would also have to engage in a time consuming process to update their privacy settings and delete outdated or inaccurate content in preparation of disclosure to CBP. Estimations that the entire processes would take anywhere between 8 and 23 minutes grossly misunderstand how social networks, privacy settings, and content sharing across the internet actually function.

Ultimately, requesting that individuals provide social media identifiers represent an overbroad and invasive request for information regarding an individual's personal and private life. CBP should be using its resources efficiently to examine concrete and accurate sources of information instead of requesting individuals disclose virtually every aspect of their online identity. Consequently, ILRC and NIPNLG reiterate their opposition to the collection of social media identifiers and strongly urge CBP to rescind this proposed collection. *Comment on CBP Collection of Social Media Identifiers [Docket No. USCIS-2016-14848; OMB Control Number 1615-0111. Page 10 of 10]*

10

Thank you for your consideration of our views. Should you have any questions regarding this comment, please feel free to contact Jose Magana-Salgado at (202) 777-8999 or [jmagana@ilrc.org](mailto:jmagana@ilrc.org).

Sincerely,

Jose Magana-Salgado

Managing Policy Attorney

Immigrant Legal Resource Center

Comment Submitted by Michael Roper

**Comment**

View document:

absolutely wrong, they should not infringe my own privacy for absolutely speculative reasons

Comment Submitted by Miguel Mercado

**Comment**

View document:

Nowadays if we post something that does not follow the opinion of others you can be considered a terrorist even if you are not one. Searching online presence would only generate more misunderstandings.

Comment Submitted by Carl Stonebraker

**Comment**

View document:

This whole idea seems to be a further violation of the constitutional right against unreasonable search and another step towards a police state. If they suspect I've committed a crime, get a search warrant. Otherwise they have NO need to access my accounts.

Comment Submitted by Hugh Peach

**Comment**

View document:

The Internet should be for free speech and creativity. But, free expression will also mean that people will sometimes be sarcastic, cynical, joke with friends, project absurd messages and engage in hyperbole. Because electronic scanning is so easy, any attempt in government monitoring in this area will be too much and easily result in the kinds of continuous bureaucratic idiocy and political repression typical of authoritarian states. This will be inherently unjust to individuals singled out by the monitoring, destructive to social trust, undermine the perceived legitimacy of government and weaken free and creative expression.

Comment Submitted by Sa McCue

**Comment**

View document:

It is a violation of free expression and free speech. To use someone's social presence and opinions against them goes against the very principles of this nation. It also reeks of martial law and the set-up of a nanny state, which is the wrong direction for a supposedly free nation.

Comment Submitted by Lauren Richard- Evans

**Comment**

View document:

I think it should only become an option because it must be noted that such personal information can be made vulnerable to hacking, and even if it does become mandatory, social media information can be misread. The DHS must be thorough in recognizing that the information given is a true threat to the country's security before taking action.

Comment Submitted by Marina Muilwijk

**Comment**

View document:

It would be a reason for me not to visit the U.S. (As a tourist or for work meetings).

Comment Submitted by Steven Shelton

**Comment**

View document:

I don't have a problem with it at all. I don't know anyone closely who would oppose having their information looked at. If I do, I don't know them well. Do I like it? There are things I like better. But I don't have a problem with it.

Comment Submitted by Rich Walker

**Comment**

View document:

It's a terrible idea that will have a chilling effect on international business and commerce.

Comment Submitted by Yolanda Rondon

**Comment**

View document:

The U.S. government has no right to invade by privacy and freedom of speech. I would have serious concerns of the government misusing information and cast me in a light of suspicion based on my constitutionally protected right to express political objection to government policies. I am not a criminal and have not committed any crimes. If the government wants access to information, they need to get a warrant and prove probable cause.

Comment Submitted by James Williams

**Comment**

View document:

The US Post Office delivers snail mail spam. I consider it my duty as a US citizen to spam Homeland Security.

Comment Submitted by Ken Martin

**Comment**

View document:

They are welcome to search my gmail online presence. I use no social media.

Comment Submitted by Carolyn Wise

**Comment**

View document:

Ridiculous, asinine, absurd, and a waste of taxpayers dollars. Things I said to a friend online as part of an ongoing joke should not be used against me, nor should views I held over a decade ago and no longer hold. This does not keep American citizens safer, it just keeps America exclusive, which is not at all the same thing and is not at all fair to anyone.

Comment Submitted by Rena Razor

**Comment**

View document:

Terrorists and associates are going to lie about social media presence, create fake profiles or simply steal someone else's online presence in order to gain access. The only ones affected will as usual, be the law abiding general public.

Comment Submitted by Ahmed Sakkal

**Comment**

View document:

Privacy and freedom of speech are protected by the constitution  
This will certainly infringe on both

Comment Submitted by Brian Laneville

**Comment**

View document:

Speech cannot be considered truly free if it is dissected in a way that may hinder an uninterrupted flow that speech. I believe the hinders free speech and unwarranted search & seizure.

Comment Submitted by Huguette Moran

**Comment**

View document:

Searching our online Presence is a direct violation of our privacy. That would be the beginning of a police state

Comment Submitted by Jessica [Last Name Unknown]

**Comment**

View document:

it's none of their business! and it would be a waste of theirs, and mine, and everyone else around's time. what friends I have, what posts I post, and messages I receive are mine and my own property. the only way it would be acceptable, is if I, in turn, could see THEIR social media accounts as well.

Comment Submitted by Dale Weingartner

**Comment**

View document:

This will be a waste of time, money and personnel and hold up the already long lines. Many times social media statements aren't true, are song lyrics and or just expressions used only among friends. They could be taken the wrong way.

Comment Submitted by Pat Turney

**Comment**

View document:

Privacy is the first order. We are protected from unreasonable invasion of privacy (from search and seizure). A court order should be obtained from a judge to prevent unreasonable privacy intrusions.

Comment Submitted by James Pannacciulli

**Comment**

View document:

This would be a massively ineffective and invasive measure which would nearly certainly be used to ethically questionable ends well beyond its presumed intent.

Comment Submitted by Rev. Bradius V. Maurus III

**Comment**

View document:

This has a chilling effect on freedom of speech and the government should be ashamed of trying to impose such a nosy system on its citizens or others. It is deeply unAmerican and repulsive. True security includes securing the individual citizen's privacy.

Comment Submitted by Harold Sharp

**Comment**

View document:

I don't use social media since I think it invades my privacy. Companies already have records of my shopping habits, and I put up with that, even though I dislike it. People post all kinds of crap on social media that can be taken out of context, which I don't believe the US government needs to determine who is or is not safe to be allowed into their country. They already have watch lists for people they suspect of various activities, but that didn't help in Orlando. It seems that adding another few million people to these lists, especially based on on the drivel posted on social media, won't help keep people safe from either terrorists or crazies.



Comment Submitted by Steve Wilson

**Comment**

View document:

Corporatism and debt slavery is all the modern USA has ever stood for. They hate the working class, they hate ordinary people and will do anything to push their fascist, racist, slaveowner agenda. Disgusting to anyone with even a shred of human decency.

Comment Submitted by Pia Rydin

**Comment**

View document:

This is my private life, not the U.S Departement, nor any other state or goverment has the right to have access to mine or any other persons private life.

Comment Submitted by William Mondale

**Comment**

View document:

I believe this reflects poorly on a nation founded on the principle of freedom of expression.

Comment Submitted by Patrick Sennello

**Comment**

View document:

Homelans Security should not be turning into a Gestapo

Comment Submitted by Copper Wiley

**Comment**

View document:

It's a gross invasion of privacy

Comment Submitted by Cameron Nicholson

**Comment**

View document:

Surveillance in this way chills free speech. It is unamerican.

Comment Submitted by Mohammad Shadmehr

**Comment**

View document:

The next step is fascism

Comment Submitted by Teodora Petersen

**Comment**

View document:

This plan is a breach of democracy.

Comment Submitted by Ken Wasch, Software & Information Industry Association

August 22, 2016

U.S. Customs and Border Protection Agency

United States Department of Homeland Security

90 K Street, NE; 10th Floor

Washington, DC 20229

**Attn: Paperwork Reduction Act Officer**

On behalf of the Software & Information Industry Association (SIIA), thank you for initiating the Request for Comment pertaining to the proposed extension and revision of information collection practices for Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization.

SIIA is the principal trade association for the software and digital information industries. The more than 700 software companies, data and analytics firms, information service companies, and digital publishers that make up our membership serve nearly every segment of society, including business, education, government, healthcare and consumers. As leaders in the global market for software and information products and services, they are drivers of innovation and economic strength—software alone contributes \$425 billion to the U.S. economy and directly employs 2.5 million workers and supports millions of other jobs.

SIIA understands and supports the goal to learn more about potential threats posed by visitors to the U.S., particularly the desire to access any information that is publicly available and could provide greater clarity and visibility to possible nefarious activity and connections. While we appreciate the exploration of voluntary sharing of additional information, we are concerned that the proposed voluntary disclosure would be perceived as a mandatory disclosure, or that the proposed disclosure could become required further in the future.

By any measure, collection of the proposed information by DHS would represent an expansion of information currently collected for visa-waiver applications, such as a person's name, address, criminal background, health status, and duration of stay. Without further consideration and greater detail, we do not believe that this policy would be helpful in achieving the goals of DHS, and it is likely to have significant negative outcomes. Following are a list of key concerns we have identified. [Software & Information Industry Association](#)

2

**The concepts such as “online presence” and “social media identifier” are neither clearly defined, nor are they practical terms to be used as categories of information gathered from individuals.**

The information and communications technology (ICT) landscape is evolving very rapidly, particularly with respect to the use of applications and services to communicate and engage in social activities. Not long ago, “social media” options were comprised of a limited number of social network services that connected individuals and enhanced digital communication, in some cases with friends, associates and colleagues, or in other cases publicly for broadcast to the general public. However, over the last several years, the social media landscape has grown exponentially beyond just a handful of network services, and many of the services are largely used for private communications with select users. Today, there are dozens of social networks and applications where individuals connect with one another over the internet to communicate and express their thoughts and feelings.

For instance, the category of leading services consists of more than 15 social media services used by millions of individuals worldwide. In addition to the most widely used such as Facebook, Twitter, YouTube and LinkedIn, other services such as Instagram, Tumblr, Pinterest, Badoo, Reddit, Quorra, Snapchat, WhatsApp and Yammer are very popular and growing in usership. These are just a handful of social media services in use today for individuals to establish an “online presence.” This handful of examples highlights the recent explosion of social media services over the last decade, and it highlights the expectations for further growth due to the increasing popularity of internet-based networking.<sup>1</sup>

1 <http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/>

2 <https://www.brandwatch.com/2016/03/96-amazing-social-media-statistics-and-facts-for-2016/>

Recent data underscores the breadth and rapid growth rate of social media, as well of the diversity of services in use today:<sup>2</sup>

□ As of July 2015, total worldwide population is 7.3 billion,

- ☐ Of the 3.17 billion internet users, there are currently approx. 2.3 billion active social media users,
- ☐ Internet users have an average of 5.54 social media accounts,
- ☐ Social media uses have risen by 176 million in the last year, and
- ☐ 1 million new active mobile social users are added every day—that's 12 each second.

In addition to the currently strong adoption of stand-alone social media services and platforms, one of the most significant developments we have been observing in the social media landscape is the adoption of social-media platforms and services within other internet-based applications and platforms, both targeted at consumers and professional users. For instance, social media platforms within online game networks or within broader business enterprise networks. The development of these types of social network services further complicates the task of identifying [Software & Information Industry Association](#)

3

a practical universe of social media, not to mention clarifying what might differentiate a “social media identifier,” from other account information for accessing a wide range of internet-based services—social networking will continue to be built into everyday citizen services, such as commerce, providing individuals the opportunity to publicly rate vendors, transactions, products and services, and to engage in digital dialogue, either public or private.

Further, many services and platforms provide a service for individuals based on a defining category. For example, many dating apps offer services to a specific demographic. Declaring use of such a particular service may reveal more about an individual than they publicly wish to, and it could lead to a belief that this factor about themselves – whether it be sexuality, religion, disability, or other defining factor – may be a discriminating factor used by the U.S. government in deciding entry to the United States.

In light of the dynamic, rapidly evolving social media landscape, it is impractical to define for policy purposes commonly used terms such as “social media identifier,” not to mention broader concepts such as “online presence.” These challenges are very real presently in 2016, and they will only increase in the years to come.

**There is a lack of clarity about the type of data that will be collected, or how it will be used, and what criteria might be used to reject entry into the United States.**

The proposal states that the information collected in this optional data field will be used for “providing another tool for investigators and analysts” to “enhance the existing investigative process” including vetting purposes for inclusion in the program by investigators and analysts. However, the policy does not elaborate on what would constitute an “identifier,” or how this new data would be used in the vetting process. The proposal is lacking critical detail around the wide range of social information that might ultimately be reviewed or collected—including potentially both personal connections and communications—and how this could be used in investigation and analysis. The proposed policy does not appear to request access to password and log-on information, which would of course be an

extremely invasive request, but it also does not preclude this from being included within the definition of “identifier.” Nor does the proposal indicate whether the providers of these services will be expected to provide additional information about their users. This would also increase the level of invasiveness, as well as being disproportionate to what the visa waiver process seeks to achieve, not to mention adding a substantial additional burden on companies, the cost of which has not been factored into the proposal.

Additionally, given that there are a limited number of applicants who are approved for the program, it would be a reasonable assumption that the refusal or failure to comply with the voluntary request for social media information could preclude the opportunity to enter into the United States, despite the information request being described as a strictly a “voluntary” disclosure. That is, applicants would reasonably assume that their chances of being admitted to the United States would be diminished if they did not provide the information, or at least that they would likely be subjected to additional questioning at the border. [Software & Information Industry Association](#)

4

At a time when there is heated political debate about discrimination of certain ethnic or religious groups for entry into the United States, we are concerned that using social media information could be used as the key tool for discrimination, e.g. to deny a waiver based on religious beliefs or undetermined ideological grounds. If DHS seeks to request this expansion of information disclosure, even voluntarily, for the vetting process for visitor entry into the United States, the proposed policies and practices associated with social media data monitoring and analysis should be more thoroughly considered and more clearly established.

**The proposal is not likely to provide an effective mechanism for useful information collection.**

In addition to the impracticality of defining what is, or is not, relevant “social media,” or the types of information collected, there are other inherent shortcomings of the proposed approach. A Government request for access to this type of personal information, even in a voluntary context, are likely to cause all users to think twice about using these services, potentially leading to an environment where users either self-censor their communications, or even limit their use of these services altogether. This would certainly be the case if the policy were to take the ill-conceived step of identifying specific social media platforms. A modification of social media usage would be a likely outcome for a wide range of users who fear an invasion of their privacy, and it would most certainly be routine for the nefarious actors that the U.S. Government is seeking to identify.

At the same time, there are significant questions about the accuracy and usefulness of the information collected. The stated goal of the new information collection is to “enhance the existing investigative process” for screening purposes. But this assumes that individuals will self-disclose information that is not only accurate, but that also could be helpful for the Government to predict the risk of nefarious actions or certain individuals are inherently more likely to engage in nefarious activities. Conversely, terrorists or other nefarious actors would be most likely to volunteer only social media information that is “clean,” disclose information that is inauthentic or even establish false accounts for the purpose of providing an alias. The ability of DHS to differentiate between authentic and inauthentic information

provided, or to attain the types of information it seeks, if even possible, would require a substantial undertaking.

Also, due to the high likelihood of typographical errors or fraudulent representations, it would be imprudent and harmful to treat a representation on a visa-waiver form of ownership over a “social media identifier” as conclusive information, particularly if this were to override authentication mechanisms in place today.

For these reasons, this policy is likely to be an expansive, ambiguous information request for millions of individuals who pose no threat to the United States, while not likely yielding meaningful information to identify real threats. [Software & Information Industry Association](#)

5

## **Conclusion**

Again, thank you for the opportunity to comment on this proposed policy. Based on the concerns identified above, we urge you to further consider the key objectives of expanding information disclosure for the visa-waiver program, the critical details of the proposed policy which are currently undetermined, and the potential ramifications this policy could have among our allies and trading partners, not to mention all other countries around the world.

Sincerely,

Ken Wasch

President

Comment Submitted by Alexa Sarten

## **Comment**

View document:

The proposed program is a horrific breach of personal privacy. Information posted anonymously or pseudonymously on the internet should not be linked by a government agency to official records.

Comment Submitted by Will Sage

## **Comment**

View document:

It should not be allowed in any form or procedure.

Comment Submitted by Sarah Tatoun

**Comment**

View document:

What an absolutely horrible idea! Are we to give up ALL our rights now to 'protect' ourselves against terrorist? As if real terrorists wouldn't know how to protect their information! The government intrusion on our lives is already verging on levels common in totalitarian states. As a US citizen married to a non-citizen I absolutely oppose any further invasions of our personal space and privacy.

Comment Submitted by Jean Stansfield

**Comment**

View document:

This is an invasion of privacy and an insult to me as a person.

Comment Submitted by Bruce Smith

**Comment**

View document:

Two foundational principles of the United States are freedom of speech, and the right to assemble, which are core components and the backbone of social media. These principles should be protected, or we as a society lose much of what makes the US such a great nation! The US needs to self-regulate; stay out of private citizen information unless a judge warrants that there is enough compelling existing information to do otherwise!

Comment Submitted by Anonymous

**Comment**

View document:

The USDHS should continue to evaluate visitors and migrants to the country on a basis of merit, not on opinions posted on fact lacking sites such as facebook and social status.

Comment Submitted by Peter Juul

**Comment**

View document:

There's a history of police forces and similar agencies making false conclusions and detaining innocents because of software gone wild or prejudices in the examining agent.

The more random information not intended for such analysis available to such agents, the higher the risk of false conclusions.

My worst fear in this is the classic case of 'the computer says we should detain/refuse you'

Comment Submitted by Kristen Lee

**Comment**

View document:

It is an abhorrent violation of privacy that screams Big Brother

Comment Submitted by Brian Jacobel

**Comment**

View document:

It's a gross invasion of privacy and won't stand up to legal challenge.

Comment Submitted by William Noffsinger

**Comment**

View document:

Invasive, Orwellian, Authoritarian, Paranoid Overreaching.

Comment Submitted by Hannah Spaulding

**Comment**

View document:

I find it intrusive and worry about the precedent it sets for other countries to do similar, and worse, based on it. Also, I can only see this adding to the 'haystack' of information and making things even more difficult.



Comment Submitted by Sterling Sheehy

**Comment**

View document:

It's bad enough that everybody has a crazy gun nut racist uncle on Facebook, the idea that our ability to travel freely simple because we were respectful and friended them on Facebook is absurd.

Comment Submitted by Thomas Lowenhaupt

**Comment**

View document:

drop the plan.

Comment Submitted by Mary Ann Peterson

**Comment**

View document:

I am 79 years old and consider myself mentally sharp for my age yet do not remember all my user names and passwords. I would have to carry a card with that info which is not a good idea. Would I be arrested if I couldn't remember? This is insane. A warrant showing probable cause should be used before any such information is required.

Comment Submitted by Phoebe McLeod

**Comment**

View document:

This is an invasion of my personal privacy, and I don't think it should be allowed.

Page 7

Comment Submitted by Christian Massot

**Comment**

View document:

Online presence should not be systematically searched only in case of criminal investigation

Comment Submitted by Joseph Scott

**Comment**

View document:

By its very nature, social media is not and cannot be private. But any law that must be enforced in secret is not a law.

Comment Submitted by Isabel San Gabino

**Comment**

View document:

Freedom is based in education, development and cooperation. Mass surveillance is of no use to prevent an attack but is a big loose of freedom.

Comment Submitted by Benjamin Kreuter

**Comment**

View document:

As someone who has a deliberately limited online presence, I am concerned that my lack of social media accounts will be taken to be a refusal to submit this information. What is officially voluntary is often not so voluntary in practice and what officially will not be considered suspicious is often considered so in practice. I am also disturbed by the idea that a handful of large corporations will be given such a role in deciding who can enter our nation.

Comment Submitted by Marc Loehrwald

**Comment**

View document:

Whatever I post online does belong to me and I decide to whom I'll share it with!

Comment Submitted by Diogo Marques

**Comment**

View document:

Clear violation of free space and right to assembly. If a specific person is suspected of association with criminal elements the justice system provides warrants for search a seizures. A dragnet is unnecessary burden on the people.

Comment Submitted by James Thomas

**Comment**

View document:

No!

Comment Submitted by Terry Thrasher

**Comment**

View document:

If you wish to search any online presence you must do it from a similarly situated position, who is searching, why, and only done with permission. No representatives, no fake accounts, if you can't be open and transparent don't do it at all.

Comment Submitted by Tammy Thompson

**Comment**

View document:

I think to require it is an invasion of privacy. However, we all know nothing is really private on the internet, if Homeland security or any agency for that matter wants to spy on people I suggest they hire hackers to do it the old fashion way and find a non-taxpayer way to pay for it.

Comment Submitted by Elizabeth Stewart

**Comment**

View document:

PRIVACY.

Comment Submitted by L Marks

**Comment**

[View document:](#)

The department should collect, or spend any money collecting social media information. The department needs to be as transparent as possible both with citizens and visitors to our country. Gathering more personally identifiable information and indexing it is the wrong direction for border patrol.

Comment Submitted by L Tin

**Comment**

[View document:](#)

The US just dropped even lower on my list of places to visit or have any business with.

Comment Submitted by Diane Spiller

**Comment**

[View document:](#)

This would be a ridiculous waste of time, money and effort. It would not prevent terrorist attacks and would inconvenience millions of people.

Comment Submitted by Mark Langford

**Comment**

[View document:](#)

It is an invasion of my privacy, irrelevant to any reason I may choose to enter the US. There is no more reason to check my online presence than there is to check my primary school reports or the contents of my waste paper bin. Using my online presence to determine my fitness for entry is to deny me my right to freedom of expression and freedom of speech, a freedom supposedly guaranteed by the First Amendment to the US constitution.

On the other hand, if the US Government were to start demanding that entrants to the US hand over their social presence on entry, you can be certain that other countries will do the same to US visitors...

Comment Submitted by Rob MacArthur

**Comment**

[View document:](#)

Not only is this a violation of the inalienable human right to privacy, it is enormously wasteful of time and money.

Comment Submitted by David Kallechey

**Comment**

View document:

Unconstitutional. This is none of their business. This a violation of our privacy.

Comment Submitted by John West

**Comment**

View document:

I have no problem if there is reasonable suspicion and a warrant has been obtained from a federal judge based on any information that has raised Homeland Security's suspicion. Otherwise they should not have the right to request this information from any passenger entering the United States.

Comment Submitted by Volker Leimann

**Comment**

View document:

The increasing fascism what the evil US-Empire is forcing on the world is repugnant.

Comment Submitted by Travis Vick

**Comment**

View document:

It is unfortunate in a way that that many aspects of peoples private life have been subsumed by the technological tide that is social media & the internet. Conversations & ideas that at one time would have been shared in good natured company over cups of coffee & late night meals are now shared on the 'private' walls of friends social media feeds. The dialog & course correction that would arise from these

intellectual (sometimes quasi-intellectual) debates is the meat that forms the base of a well rounded world view. Ideologies & policy points are debated & shifted in this environment.

Other aspects of life, however shift too. Such as the forum in which these conversations take place. The openness of the diner's booth, coffee shop or backyard deck have to some extent been replaced by the digital canvas of social media. If you wish to engage with your increasingly dispersed peers, you must do it online if you want to be part of wider, bolder & better informed citizenry. Conversations that may contain ill-formed ideas or positions or dangerous counterpoints in debate, 25 years ago would have been free to take place in those afore-mentioned locations without outside, context-less interrogation.

Searching & recording the online presence of individuals who are not part of an ongoing specific investigation is the equivalent of wiretapping every person, retroactively, upon entering or re-entering the United States, & is an implicit threat to free speech and the ability to have open dialog without fear of reprisal. Not too mention the incidental invasions of privacy concerning medical, legal & other matters that were presumed to be discussed in confidence or anonymity.

I add my comments & proudly attach my name to them, with no screen of anonymity. I believe wholeheartedly what I stated above & have confidence that if enough Americans speak out against un-American ideas such as those proposed by the DHS & Customs agencies some sanity can be injected into pol...

Comment Submitted by Grant Meadors

**Comment**

View document:

Please do not collect this information. It is unethical, invasive, impractical.

Comment Submitted by Peter Jespersen

**Comment**

View document:

It is worthy a military dictatorship

Comment Submitted by Emilie Nouveau

**Comment**

View document:

I think this only harms decent citizens. It limits expression and would likely create a feeling of paranoia around social media posting and connecting. Anyone who is actively engaged in harmful activities would

be prepared with a safe looking social media account, so all this would accomplish is making the average citizen uncomfortable.

Comment Submitted by Bo Link

**Comment**

View document:

This is completely ridiculous that you all are even thinking about this.

Comment Submitted by Kathleen Pickard

**Comment**

View document:

That is a huge waste of time and money. Terrorists will know how to get around it so you will only be harrassing ordinary citizens who have done nothing wrong.

Comment Submitted by Dael Jackson

**Comment**

View document:

As someone who travels abroad a lot, I deeply fear other governments will use reciprocity rules to investigate my social media. This is a wrong policy that will not keep anyone safe. It instead is expensive security theater that will expose my personal data to other governments.

Comment Submitted by H. J. Kooy

**Comment**

View document:

Do they want to become my friend online?  
Are they clearing me for this job that requires clearance, and if so... did I get the job?

Comment Submitted by Ingo Lembcke

**Comment**

View document:

Close your borders and do not let anyone enter! Else, this is a bad idea.

Comment Submitted by Janiece Staton

**Comment**

View document:

This is incredible over-reach, not to mention invasive and unnecessarily intrusive! The sick & twisted law enforcement snoops who can't think of anything better to do with their work hours than come up with evermore creepy ways to spy on the private lives of Americans need to be fired, as they're clearly not using their time effectively, nor viewing their fellow citizens with any degree of respect! If they want to spy on my private life, I should be given all of their social media records and lists of personal friends and relations to inspect, long before they get to see mine!

Comment Submitted by Maria Studer

**Comment**

View document:

Homeland Security should not be able to search anyone's online presence without a warrant signed by a judge.

Comment Submitted by Ewen Kloas

**Comment**

View document:

Totalitarianism. George Orwell's 1984 is upon us.

Comment Submitted by Olh Katalin

**Comment**

View document:

Although I don't care, what anyone thinks about my social media activity, it should not be considered when I apply for an entry visa to the USA.

Comment Submitted by Angela [Last Name Unknown]

**Comment**



View document:

If this becomes law for visitors entering the US, how long will it be before it becomes law for everyone living in the US, citizen, legal alien, or illegal alien? I oppose with every fiber of my being this invasive policy, and will vote for Congresspeople who also oppose it/vote against candidates who support it.

Comment Submitted by Jonathan Sweet

**Comment**

View document:

It's disgustingly invasive.

Comment Submitted by Eric Ranvig

**Comment**

View document:

The U.S. Department of Homeland Security should seek a search warrant for probable cause, if they suspect a passenger of criminal wrong doing. Otherwise, they should not have the right to search personal social media or email accounts.

Comment Submitted by Daniela Ruegg

**Comment**

View document:

very invasive of people privacy, not everyone is a terrorist and people shouldn't be judged a security risk without having had some criminal precedents

Comment Submitted by Diana Sierras

**Comment**

View document:

I think it would be a terrible breach of privacy, something that would happen in Russia, China, North Korea, etc. We are a free and open society and must devise other means to keep ourselves safe in this turbulent world, but police-state tactics are not the answer.

Comment Submitted by Robert Lyle

**Comment**

View document:

Once this kind of information is gathered, even on the most innocent of us, we could be subject to government intervention/arrest for any political opinions we hold. It would be a very dangerous start down a very slippery slope.

Comment Submitted by Joe McMahon

**Comment**

View document:

This is a pointless exercise, as anyone who doesn't want the TSA sifting around in their data will simply provide them with a dummy account. If this goes into law, any international traveller will simply hand you a dummy account and not reveal their primary account. If the law is worded such that all accounts must be revealed, then any bad actors will simply lie. This is a pointless exercise which will build yet another database full of personally-identifying information that will sooner or later be leaked, stolen, or otherwise exploited.

Comment Submitted by Alun Phillips

**Comment**

View document:

Wow, what a pointless trawl. What makes you think terrorists intent on terrorism would not set up a clean account to escape notice?

Comment Submitted by Hermann Romuss

**Comment**

View document:

Land of the free? As long as you do exactly as you are told. No thank you. I rather not visit the U.S.

Comment Submitted by Vince Mendieta

**Comment**

View document:

More crap from McCarthyites.

Comment Submitted by John and Martha Stoltenberg

**Comment**

View document:

Stop and reverse the rise of fascism in capitalist America! Stop and reverse the rise of the American fascist capitalist military/police state!

Comment Submitted by Anne Cecilie Rohweder

**Comment**

View document:

Not to trust have confidence in humans is the surest and most expensive road to conflict, but it is difficult, because so many people are employed and depending on conflicts and fabricating weapons. And the warindustry even neutral countries like Sweden participate in. All this people and countries do not want confidence they are depending on distrust.

Comment Submitted by Lorna Will

**Comment**

View document:

I think this is a gross invasion of the little privacy we have left.

Comment Submitted by James Marshall

**Comment**

View document:

Requiring social media data is a terrible idea, from a security standpoint. Social media is already a security nightmare, and any access the USG gets will surely spread to other, less benevolent governments and other actors.

Comment Submitted by Michael Lampi

**Comment**

View document:

As a US citizen my online presence is only for the eyes of those I choose. It is not for the eyes of anyone else, and I would consider it to be a gross invasion of my privacy for anyone - including the US Department of Homeland Security - to search my online presence at any time.

Comment Submitted by Gini [Last Name Unknown]

**Comment**

View document:

Good thing that most of the wannabe terrorists are even dumber than this idea.

Comment Submitted by Chris Weigert

**Comment**

View document:

I think it's a horrific blow to free assembly and association, not to mention a gross invasion of privacy.

Comment Submitted by Christopher Turnbow

**Comment**

View document:

Knowing that a government agency with authority to act at its own discretion has the ability to monitor what a person says in any forum, has a chilling effect on free speech. I do not believe that my government needs this power in order to do its job.

By no means should we permit fear to compromise the principles of freedom. The inability to monitor what everyone is saying / posting / etc., is, to quote Jefferson, formidable to tyrants only.

I have confidence that Homeland Security can do an effective job without requiring the social media account information of people entering our country.

Comment Submitted by Rod Mathews

**Comment**

View document:

There are plenty of other countries to visit. Why should I bother with the USA. I certainly will not be if they go ahead with this.

Page 8

Comment Submitted by Gary Molen

**Comment**

View document:

Best solution: Do away with Homeland Security and all of its off shoots.

Comment Submitted by Matthew Seidl

**Comment**

View document:

I don't have any social media accounts outside of linked in. And I don't think this should penalize me. If I have to, I can open up an empty facebook account and never use it, but somehow I don't think that will satisfy boarder patrol.

Comment Submitted by Martin Nicholls

**Comment**

View document:

Are terrorists really likely to supply an incriminating social media account, when it is so trivial to create a separate benign account. This policy would be a useless waste of time and money.

Comment Submitted by Martin Nicholls

**Comment**

View document:

Are terrorists really likely to supply an incriminating social media account, when it is so trivial to create a separate benign account. This policy would be a useless waste of time and money.

Comment Submitted by Ole Seifert

**Comment**

View document:

Social Media do not necessary show the whole or true picture and its contents is easily taken out of context. Do a machine understand sarcasm or irony? Do the people who eventually read it understand it? Really?

Let privacy be privacy - do not act as a police state or a totalitarian state!

Comment Submitted by Cole Perry

**Comment**

View document:

It is a terrible idea to search people's online presence every time they enter the country. Most of most people's entire lives are online.

Comment Submitted by Sophia Cope, Electronic Frontier Foundation

August 22, 2016

**VIA REGULATIONS.GOV**

U.S. Customs and Border Protection

Attn: Paperwork Reduction Act Officer

Regulations and Rulings, Office of Trade

90 K Street, N.E., 10th Floor

Washington, DC 20229-1177

***RE: Electronic Frontier Foundation Comments on Proposed Collection of Social Media Identifiers Via Electronic System for Travel Authorization (ESTA) and Form I-94W for Visa Waiver Program Visitors to the United States***

***Docket No. USCBP-2007-0102***

***OMB No. 1651-0111***

To Whom It May Concern:

The Electronic Frontier Foundation (EFF)<sup>1</sup> submits these comments to convey our objections to Customs and Border Protection's (CBP) proposal to ask aliens seeking to enter the United States under the Visa Waiver Program (VWP) for their social media handles.

Specifically, CBP proposes to instruct VWP visitors to provide "information associated with your online presence—Provider/Platform—Social media identifier."<sup>2</sup> CBP asserts that it would be "optional" to provide this information to the U.S. government electronically via the Electronic System for Travel Authorization (ESTA) before embarking on travel to the U.S. without a visa, or via the I-94W paper form. CBP's goal in seeking this information would be to provide its parent agency, the Department of Homeland Security, "greater clarity and visibility to possible nefarious activity and connections" for "vetting purposes." CBP is seeking comments, in part, on "whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility." We argue that it would not.

**The proposal would be ineffective at protecting homeland security.** CBP's

proposal to instruct VWP visitors to disclose their social media identifiers is undoubtedly

<sup>1</sup> EFF is a San Francisco-based, non-profit, member-supported digital rights organization. As recognized experts focusing on the intersection of civil liberties and technology, EFF actively encourages and challenges

industry, government, and the courts to support free expression, privacy, and openness in the information

society. Founded in 1990, EFF has over 25,000 dues-paying members.

<sup>2</sup> 81 Fed. Reg. 40892 (June 23, 2016), <https://federalregister.gov/a/2016-14848>.

August 22, 2016

Page 2 of 9

backed by a salutary motive to prevent terrorist attacks and other harm to Americans. The proposal was likely spurred by the discovery after-the-fact that Tashfeen Malik, one of the San Bernardino shooters, expressed on Facebook her support for the Islamic State group. Presumably, CBP/DHS would use disclosed social media handles to peruse *publicly* available posts on Facebook, Twitter, Instagram and other social media platforms for evidence of terrorist intentions, affiliations or sympathies, and then deny entry based on that information. However, Ms. Malik, who was in the U.S. on a fiancée visa, expressed such sentiments in *private* messages to her Facebook friends.<sup>3</sup> She did not do so in public posts prior to the attack, according to the FBI.<sup>4</sup> The government would not have access to private messages and posts by simply knowing applicants' social media handles.<sup>5</sup> Additionally, when Ms. Malik publicly declared allegiance to ISIS on Facebook after the attack began, she did so under a pseudonymous profile.<sup>6</sup> It is highly unlikely that would-be terrorists seeking to enter the U.S. would disclose their social media identifiers—whether pseudonymous or using their real names—to CBP that reveal publicly available posts expressing support for terrorism. It is far more likely that terrorists would create secondary social media profiles that contain benign public posts, and share those handles when applying to enter the U.S.—or share none at all.

**The proposal contains no standards to ensure that innocent travelers would**

**not be misjudged and denied entry into the U.S.** Even if VWP visitors were to disclose their actual or primary social media identifiers to CBP, the proposal does not state what standards the government would use to evaluate public social media posts and ensure that innocent travelers are not denied entry into the U.S. In the past, CBP has taken posts out of context and misunderstood their meaning. In 2012, for example, Irish national Leigh Van

Bryan was denied entry into the U.S. because he tweeted to a friend: "Free this week, for

<sup>3</sup> Richard Serrano, "Tashfeen Malik messaged Facebook friends about her support for jihad," *Los Angeles*



*Times* (Dec. 14, 2015), <http://www.latimes.com/local/lanow/la-me-ln-malik-facebook-messages-jihad-20151214-story.html>.

4 Richard Serrano, “FBI chief: San Bernardino shooters did not publicly promote jihad on social media,” *Los*

*Angeles Times* (Dec. 16, 2015), <http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html>.

5 If public social media posts or other evidence supported probable cause that an account contains evidence

of criminal activity, the government could seek a warrant from a judge to obtain private social media messages or other private content stored in the cloud by U.S. providers. *See* 18 U.S.C. § 2703; *U.S. v. Warshak*,

631 F.3d 266 (6th Cir. 2010).

6 Tami Abdollah, “Facebook exec says Tashfeen Malik posted ISIS praise during San Bernardino shooting spree,” *Associated Press* (Dec. 4, 2015),

[http://www.mercurynews.com/california/ci\\_29202959/facebookexec-](http://www.mercurynews.com/california/ci_29202959/facebookexec-says-tashfeen-malik-posted-isis-praise)

[says-tashfeen-malik-posted-isis-praise](http://www.mercurynews.com/california/ci_29202959/facebookexec-says-tashfeen-malik-posted-isis-praise); Julia Greenberg, “San Bernardino suspect posted an ISIS pledge to Facebook after shooting began,” *Wired* (Dec. 4, 2015), [https://www.wired.com/2015/12/after-](https://www.wired.com/2015/12/after-sanbernardino-shooting-began-suspect-posted-isis-pledge-to-facebook/)

[sanbernardino-shooting-began-suspect-posted-isis-pledge-to-facebook/](https://www.wired.com/2015/12/after-sanbernardino-shooting-began-suspect-posted-isis-pledge-to-facebook/).

EFF Comments on CBP Social Media Identifier Proposal

August 22, 2016

Page 3 of 9

quick gossip/prep before I go and destroy America.”<sup>7</sup> Apparently it was lost on border agents that Mr. Van Bryan was using slang and humor to convey his hope that he would have a good time visiting Los Angeles. It is likely that the government would similarly misconstrue the social media posts of other innocent travelers if they were to provide their social media handles under the proposal.

Additionally, CBP has not explained how the government would avoid using social media posts to exclude individuals who might disagree with American foreign policy but who have no intention of committing violent acts. The U.S. has a disturbing history of

ideological exclusion and the proposal does nothing to ensure that this would not happen in the future.<sup>8</sup>

**The proposal would violate the privacy and freedom of speech of innocent**

**travelers and their American associates.** Universal human rights, long recognized by the United States and codified in the First and Fourth Amendments, include freedom of speech and privacy for individuals.<sup>9</sup> Yet CBP's proposal to instruct VWP visitors to disclose their social media identifiers would intrude upon these fundamental rights.

While unlikely to uncover those with actual malevolent intent, the vague and overbroad proposal would result in innocent travelers disclosing a whole host of highly personal details. The proposed language confusingly seeks "information associated with your online presence—Provider/Platform—Social media identifier." Some people would likely interpret this instruction to include all manner of online accounts, far beyond "social media." Other people may interpret it to include passwords as well as identifiers, enabling the U.S. government to easily access private content. Even if travelers disclose only their social media handles, this can easily lead the government to information about their political leanings, religious affiliations, reading habits, purchase histories, dating preferences, and sexual orientations, among other things. Moreover, given the highly networked nature of social media, the government would also learn such personal details about travelers' family members, friends, professional colleagues, and other innocent

7 Kashmir Hill, "Did U.K. Tourists Deported Due To Tweet About 'Destroying America' Get Pranked?," *Forbes*

(Jan. 30, 2012), <http://www.forbes.com/sites/kashmirhill/2012/01/30/u-k-tourists-deported-due-to-tweetabout-destroying-america/#16f9f92b32b4>.

8 See, e.g., Sheldon Chad, "Ramadan's visa ban lifted," *The Guardian* (Jan. 23, 2010), <https://www.theguardian.com/commentisfree/belief/2010/jan/23/tariq-ramadan-clinton-visa>; American

Association of University Professors, "Administration Will Address Ideological Exclusion" (Jan. 13, 2011), <https://www.aaup.org/AAUP/newsroom/prarchives/2011/ACLUjanlet.htm>.

9 See Universal Declaration of Human Rights, arts. 12, 19 (Dec. 10, 1948), [http://www.un.org/en/universaldeclaration-](http://www.un.org/en/universaldeclaration-human-rights/)

[human-rights/](http://www.un.org/en/universaldeclaration-human-rights/). Article 12 states, in part, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence....” Article 19 states, “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive

and impart information and ideas through any media and regardless of frontiers.”

EFF Comments on CBP Social Media Identifier Proposal

August 22, 2016

Page 4 of 9

associates, many of whom may be U.S. citizens and/or residents with constitutional and statutory rights.

Additionally, CBP’s proposal would chill the free speech of VWP visitors. Unwilling to share such intimate details with CBP, many innocent travelers would engage in selfcensorship, cutting back on their online activity (or deleting it altogether)<sup>10</sup> out of fear of being wrongly judged by the U.S. government. Visitors may fear that the government would use this information against them not just during the entry vetting process, but also in other unknown and future contexts. For example, today’s VWP visitors may become tomorrow’s legal permanent residents or naturalized citizens.<sup>11</sup> Or they may forgo visiting the U.S. altogether, impacting their ability to travel, and also preventing the U.S. economy from benefiting from international commerce and tourism.

Importantly, many VWP visitors have legitimate reasons for being pseudonymous online—publicly active but privately unknown—in their home countries. They may be activists or political dissidents who fear being ostracized by their communities, persecuted by their governments, or even killed for their beliefs and activities.<sup>12</sup> Once VWP visitors disclose their pseudonymous social media identifiers to the U.S. government, those accounts would forever be associated with their real, passport-verified identities. CBP has not explained how it would protect the online identities of vulnerable travelers, thereby placing their physical safety as well as their privacy and freedom of speech at great risk.

**The proposal is inconsistent with the U.S. government's promotion of Internet**

**freedom around the world.** CBP's proposal to instruct VWP visitors to disclose their social media identifiers—and the attendant risks to privacy, free speech, the ability to travel, and the personal safety of innocent travelers—is inconsistent with the U.S.

government's long-standing promotion of global Internet freedom. The U.S., of course, has

10 *See supra* n. 7. Mr. Van Bryan's experience with CBP inspired him to make his Twitter account private,

affecting his ability to engage in public conversations and debates, even in his home country.

11 Consider the pre-social media case of the "L.A. Eight," where the U.S. government sought to deport two U.S.

residents who exercised their First Amendment right to lobby against the Israeli occupation of Palestine. *See*

Neil MacFarquhar, "U.S., Stymied 21 Years, Drops Bid to Deport 2 Palestinians," *New York Times* (Nov. 1, 2007), <http://www.nytimes.com/2007/11/01/us/01settle.html>.

12 *See* David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of*

*opinion and expression on the use of encryption and anonymity to exercise the rights to freedom of opinion and*

*expression in the digital age*, [A/HRC/29/32] at 3 (May 22, 2015) ("Encryption and anonymity, today's leading

vehicles for online security, provide individuals with a means to protect their privacy, empowering them to

browse, read, develop and share opinions and information without interference and enabling journalists, civil

society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."), <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>,

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf>.

EFF Comments on CBP Social Media Identifier Proposal

August 22, 2016

Page 5 of 9

long supported universal human rights.<sup>13</sup> In 2006, former Secretary of State Condoleezza

Rice established the Global Internet Freedom Task Force to focus on human rights and the Internet specifically.<sup>14</sup> Secretary of State Hillary Clinton gave a sweeping speech on Internet freedom in 2010.<sup>15</sup> And current Secretary of State John Kerry said in 2015, “We believe people are entitled to the same rights of free expression online as they possess offline.”<sup>16</sup> The State Department continues to actively promote Internet freedom today.<sup>17</sup> So it is troubling that another arm of the federal government (CBP, under the Department of Homeland Security) has proposed a policy that would not only undermine the Internet freedom of innocent visitors to the U.S., but do little or nothing to actually protect Americans from terrorism and other threats to homeland security.

**The proposal is “optional” in name only.** It is unlikely that VWP visitors would view the request for social media identifiers as truly voluntary, thereby exacerbating the negative impacts on innocent travelers. Rather, innocent travelers would likely feel coerced to provide such information to the U.S. government and thereby be forced into the impossible choice of abridging their own privacy, engaging in self-censorship, or forgoing travel to the U.S. altogether.<sup>18</sup> Additionally, CBP has not explained how it would ensure that border agents do not punish VWP visitors for declining to disclose social media handles, for example, by extensively interrogating them or otherwise subjecting them to invasive secondary screening.

**The proposal would spur reciprocity by other nations, leading to violations of Americans’ civil liberties overseas.** Should CBP move forward with its proposal to instruct VWP visitors to disclose their social media identifiers, there would surely be a great risk of other governments acting in a similar manner. Other countries may even require that visiting U.S. persons provide detailed information about their online

<sup>13</sup> See, e.g., International Covenant on Civil and Political Rights, <https://www.congress.gov/treatydocument/>

[95th-congress/20](https://www.congress.gov/treatydocument/95th-congress/20) (signed by the U.S. in 1977 and ratified by the Senate in 1992).

<sup>14</sup> U.S. Dept. of State, *Global Internet Freedom Task Force*, Archive (Jan. 20, 2001-Jan. 20, 2009), [http://2001-](http://2001-2009.state.gov/g/drl/lbr/c26696.htm)

[2009.state.gov/g/drl/lbr/c26696.htm](http://2001-2009.state.gov/g/drl/lbr/c26696.htm).

15 U.S. Dept. of State, *Remarks of Secretary of State Hillary Rodham Clinton on Internet Freedom*, The Newseum,

Washington, D.C. (Jan. 21, 2010),

<http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>.

16 U.S. Dept. of State, *Secretary Kerry Delivers a Speech About Internet Freedom and Cybersecurity Before an*

*Audience at Korea University* (May 18, 2015), [http://www.humanrights.gov/dyn/2015/05/secretary-kerrydelivers-](http://www.humanrights.gov/dyn/2015/05/secretary-kerrydelivers-a-speech-about-internet-freedom-and-cybersecurity-before-an-audience-at-korea-university/)

[a-speech-about-internet-freedom-and-cybersecurity-before-an-audience-at-korea-university/](http://www.humanrights.gov/dyn/2015/05/secretary-kerrydelivers-a-speech-about-internet-freedom-and-cybersecurity-before-an-audience-at-korea-university/).

17 U.S. Dept. of State, Bureau of Democracy, Human Rights and Labor, *Internet Freedom*, HumanRights.gov,

<http://www.humanrights.gov/dyn/issues/internet-freedom.html>.

18 By way of comparison, in 2014, police officers in Illinois often asked individuals during traffic stops for consent to search their vehicles. Even though motorists had a right to refuse, they “consented” 88 percent of

the time (21,365 consents out of 24,240 requests). Illinois Department of Transportation, *Illinois Traffic Stop*

*Study, 2014 Annual Report*, at 11, <https://idot.illinois.gov/Assets/uploads/files/Transportation-System/Reports/Safety/Traffic-Stop-Studies/2014/2014%20ITSS%20Executive%20Summary.pdf>.

EFF Comments on CBP Social Media Identifier Proposal

August 22, 2016

Page 6 of 9

activities.<sup>19</sup> Should CBP ever expand the program beyond visa waiver countries, those with questionable or poor human rights and Internet freedom records would likely be eager to ask the same question of Americans.<sup>20</sup> This would unnecessarily put Americans at risk of being denied entry, or if granted entry, subject to surveillance and excessive scrutiny while traveling abroad.

**The proposal may inspire more serious CBP invasions into the private lives of innocent travelers, including Americans.** CBP’s proposal to instruct VWP visitors to disclose their social media identifiers is just the latest effort in a broader CBP strategy to scrutinize the digital lives of innocent travelers—foreigners and Americans alike—and it

may inspire further CBP violations of privacy and First Amendment rights.

The Department of Homeland Security launched a social media monitoring program in 2010.<sup>21</sup> Two years later, concerned members of the House of Representatives held a hearing<sup>22</sup> where DHS testified that “components of DHS such as U.S. Customs and Border Protection ... have the authority to engage in law enforcement activities which may include the use of online and Internet materials,” but the testimony did not go into detail about what this means.<sup>23</sup>

Additionally, CBP issued a policy in 2009 related to border searches of electronic devices such as cell phones, laptops and cameras possessed by *anyone* entering or leaving

19 See, e.g., Jane Engle, “Responses abroad to new U.S. entry rules have been low-key,” *Los Angeles Times* (Feb.

22, 2004), <http://articles.latimes.com/2004/feb/22/travel/tr-insider22> (“The principle of reciprocity, which

has long governed visa policies, also discourages over-retaliation. Countries that restrict entry or raise fees

for visitors risk having other countries do the same to their citizens.”); Larry Rohter, “U.S. and Brazil

Fingerprinting: Is It Getting Out of Hand?,” *New York Times* (Jan. 10, 2004),

<http://www.nytimes.com/2004/01/10/world/us-and-brazil-fingerprinting-is-it-getting-out-of-hand.html>.

20 See Freedom House, *Freedom on the Net 2015*, [https://freedomhouse.org/report/freedom-net/freedomnet-](https://freedomhouse.org/report/freedom-net/freedomnet-2015)

2015. Compare U.S. Dept. of State, *Visa Waiver Program*,

<https://travel.state.gov/content/visas/en/visit/visa-waiver-program.html> (South Korea is considered “partly free” in terms of Internet freedom and is also a visa waiver country).

21 Dept. of Homeland Security, *Privacy Compliance Review of the NOC Publicly Available Social Media Monitoring and Situational Awareness Initiative*, at 1 (May 21, 2015),

<https://www.dhs.gov/sites/default/files/publications/privacy-pcr-mmc-7-20150521.pdf>.

22 House of Representatives, Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence, *Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and*

*Ensuring Privacy* (Feb. 16, 2012), <https://homeland.house.gov/hearing/subcommittee-hearing-dhsmonitoring->

[social-networking-and-media-enhancing-intelligence/](#).

23 *Written Testimony of Mary Ellen Callahan, Chief Privacy Officer, and Richard Chávez, Director, Office of*

*Operations Coordination and Planning, U.S. Dept. of Homeland Security, for House of Representatives, Homeland*

*Security Committee, Subcommittee on Counterterrorism and Intelligence, Hearing on DHS Monitoring of Social*

*Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy*, at 9 (Feb. 16, 2012),

<https://homeland.house.gov/files/Testimony-Callahan-Chavez.pdf>. See generally Electronic Privacy

Information Center, *EPIC v. Department of Homeland Security: Media Monitoring*,

<http://epic.org/foia/epic-vdhs->

[media-monitoring/](#).

EFF Comments on CBP Social Media Identifier Proposal

August 22, 2016

Page 7 of 9

the U.S.<sup>24</sup> While it might reasonably be assumed that such searches are limited to data that is on the devices themselves (e.g., photos on a camera or computer hard drive), CBP’s policy does not include any limitations on the scope of access.<sup>25</sup> With modern smartphones, information stored in the “cloud”—on the Internet and not on the device itself—is easily accessible with the tap of a finger on an “app” icon. As the Supreme Court recently explained, “Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.”<sup>26</sup>

Should CBP establish a formal policy of instructing VWP visitors to disclose their social media identifiers—which by definition are tied to accounts in the cloud—there surely would be the temptation in the future to expand the scope of *who* is subject to the policy and/or *what data* is collected or accessed, in addition to making disclosure explicitly mandatory. It would be a series of small steps for CBP to require *all* those seeking to enter the U.S.—both foreign visitors and U.S. citizens and residents returning home—to disclose



their social media handles to investigate whether they might have become a threat to homeland security while abroad. Or CBP could subject both foreign visitors and U.S. persons to invasive *device* searches at ports of entry with the intent of easily accessing *any and all* cloud data; CBP could then access both public and private online data—not just social media content and contacts that may or may not be public (e.g., by perusing a smartphone’s Facebook app), but also other private communications and sensitive information such as health or financial status.

**Expanding CBP’s “social media” policy to include U.S. persons and/or all cloud data via searches of personal devices at the border would further burden**

**constitutional rights.** The First Amendment right to freedom of speech includes the right to associational privacy.<sup>27</sup> CBP’s current practice of searching digital devices, even if limited to data stored on the devices themselves, burdens this freedom of association. It also intrudes upon the First Amendment right to freedom of the press.<sup>28</sup> Unfettered government access to social media and other communications accounts based in the cloud that include

24 *CBP Directive No. 3340-049, Border Search of Electronic Devices Containing Information* (Aug. 20, 2009),

[https://www.dhs.gov/sites/default/files/publications/privacy\\_pia\\_cbp\\_laptop.pdf](https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_laptop.pdf).

25 *See supra* n. 24, § 3.2, Definition of “Electronic Device”: “Includes any devices that may contain information,

such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and

other media players, and any other electronic or digital devices.”

26 *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).

27 *See, e.g., NAACP v. Alabama*, 357 U.S. 449 (1958).

28 CBP recently tried to search the cell phones of a *Wall Street Journal* reporter, a U.S. citizen based in the

Middle East who was visiting Los Angeles for a wedding. She advised the agent of her need to protect her

confidential sources. *See* Joseph Cox, “WSJ Reporter: Homeland Security Tried to Take My Phones at the Border,” *Motherboard/Vice* (July 21, 2016), [http://motherboard.vice.com/en\\_uk/read/wsj-reporterhomeland-](http://motherboard.vice.com/en_uk/read/wsj-reporterhomeland-)

[security-tried-to-take-my-phones-at-the-border.](#)

EFF Comments on CBP Social Media Identifier Proposal

August 22, 2016

Page 8 of 9

detailed records of a traveler's contacts, both personal and professional, individual and organizational, would exacerbate such First Amendment invasions.

Additionally, courts have held in recent years that the Fourth Amendment, which guards against unreasonable searches and seizures by the government, protects personal data stored on or accessed via digital devices, including at the border.<sup>29</sup> In so holding, the courts noted the significant privacy implications of cloud computing.<sup>30</sup> In 2014, the Supreme Court held in *Riley* that a warrant based on probable cause "is generally required before ... a search [of a cell phone], even when a cell phone is seized incident to arrest."<sup>31</sup> As to cloud computing, the Court stated, "To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter... But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen."<sup>32</sup>

Indeed, the government lawyers in *Riley* "concede[d] that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud."<sup>33</sup> Thus, it is troubling that CBP now is seeking access to some foreign travelers' cloud-based social media information, at the same time CBP reserves the right to search the digital devices of all travelers, including Americans, without a warrant or any individualized suspicion.<sup>34</sup>

<sup>29</sup> Under the border search doctrine, searches generally do not require a judge-issued warrant, and "routine"

searches do not require any individualized suspicion (*i.e.*, no probable cause or reasonable suspicion that

evidence of a crime will be found). *See, e.g., United States v. Ramsey*, 431 U.S. 606 (1977). However, lower

courts have held that the Fourth Amendment requires that “forensic” computer-aided border searches of

digital devices, as opposed to “routine” manual searches, be supported at minimum by reasonable suspicion.

*See United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc); *United States v. Saboonchi* (“*Saboonchi*

”), 990 F. Supp. 2d 536 (D. Md. 2014); *United States v. Kolsuz*, 2016 WL 2658156 (E.D. Va. 2016).

30 *See, e.g., Cotterman*, 709 F.3d at 965 (“With the ubiquity of cloud computing, the government’s reach into

private data becomes even more problematic.”).

31 *Riley*, 134 S. Ct. at 2493. *See also United States v. Kim*, 103 F.Supp.3d 32, 55 (D. D.C. 2015) (discussing *Riley*

at length and stating that the Fourth Amendment analysis “does not turn on the application of an undefined

term like ‘forensic’”).

32 *Id.* at 2491.

33 *Id.*

34 *See supra* n. 24, § 5.1.2: “In the course of a border search, with or without individualized suspicion, an

Officer may examine electronic devices and may review and analyze the information encountered at the border, subject to the requirements and limitations provided herein and applicable law.”

EFF Comments on CBP Social Media Identifier Proposal

August 22, 2016

Page 9 of 9

\* \* \*

In summary, EFF respectfully recommends that CBP withdraw the present proposal to instruct Visa Waiver Program visitors to disclose their social media identifiers.

Sincerely,

/s/

Sophia Cope

Staff Attorney

Electronic Frontier Foundation

415-436-9333 Ext. 155

[sophia@eff.org](mailto:sophia@eff.org)

Comment Submitted by Nemat Sarnevesht

**Comment**

View document:

Stay the hell out of my private life.

Comment Submitted by William Saenz

**Comment**

View document:

Dangerous and unnecessary mission creep.

Comment Submitted by Jord Swart

**Comment**

View document:

Stasi tactics. I am already trying to avoid visits to the US, these tactics will make that situation worse.

Comment Submitted by Edh Stanley

**Comment**

View document:

Big Brother is on social media....

Comment Submitted by Lisa Smeraldi

**Comment**

View document:

This is not how you protect your citizens

Comment Submitted by Aamu Kurko

**Comment**

View document:

Orwell.

Comment Submitted by Kris Lee

**Comment**

View document:

A person should not be unfairly judged based on the contacts that he/she has on social media - those may be casual followers or acquaintances whom the person do not even know in depth.

Comment Submitted by Erma Lowe

**Comment**

View document:

Every citizen has an innate right to privacy. If the US Government believes that certain social media sites are dangerous, they should monitor those sites. If a person entering the US has been found to have questionable posts to a site that been determined to be dangerous, probable cause is therefore in place to give the government the right to further question that person. Rules of Habeus Corpus, and personal civil rghts should always be respected.

Comment Submitted by Patti Martin

**Comment**

View document:

FREEEEEEEDOOOOMMMMMM! I do believe it was what William Wallace screamed as he was MURDERED for freedom.

Comment Submitted by Edward Kowalski

**Comment**

View document:

if I was concerned about government(s) knowledge of my opinions, I wouldn't be able to think - much less post them.

B) bwaaahahahah! They can't even keep their internal systems running (multiple projects trying to come up to speed (SSA, IRS, way too many DoD programs)

C) always follow the money - who is going to get richer by implementing this?

Comment Submitted by John Markham

**Comment**

View document:

This is a violation of free speech, and is very Orweillian. This is a horrible idea.

Comment Submitted by Michael Thompson

**Comment**

View document:

I'm not on Facebook, I have never tweeted. I simply don't see the point. Now that could make me look suspicious!

Comment Submitted by Anonymous (the people united)

No gods, no masters, no nations, no borders. We are not one nation under God, we are one people under the same sky, and we all must have the same rights, one of those being the right to travel where we want without being treated like criminals simply for travelling. No person is illegal. Immigration is something all people should have the freedom to do, whenever they please. No longer should nations steal the labor and wealth of the masses and then use it to defend themselves from the consequences of their actions. Open the border, open all borders across the world, and give people back the wealth that was taken from them by force through imperialism, colonialism, and capitalism.

Comment Submitted by Nathalie Marechal

**Comment**

View document:

The chilling effects this would have on free expression would be catastrophic. US leadership means that we should be prepared for any country in the world to institute similar policies to ours, including countries that are actively hostile to human rights and/or to US national interests. This is a troubling, un-American proposal - a phrase I do not use lightly.

Comment Submitted by Kevin Tims

**Comment**

View document:

No thank you ....

Comment Submitted by Kirron Welch

**Comment**

View document:

what has your social life got to do with entry into a country it has not been there before and Millions of people enter the states each year with no incidents. What would be the criteria of you being restricted access, can we also ask to see the social media sites of those FBI agents and TSA staff and the Airport staff that will be making these decisions, if we are opening this up then we should be able to see the social sites of all airport staff that interact with us as well.

Comment Submitted by Kate Lindstrom

**Comment**

View document:

I think it is a serious privacy violation. The dept of Homeland Security seems to have forgotten that government works for the people, not vice versa.

Comment Submitted by Phillip Pflager

**Comment**

View document:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Comment Submitted by Esther Kirk

**Comment**

View document:

I am entitled to life, liberty, and the pursuit of happiness. I am entitled to privacy. Our government should not be the Gestapo! They have no right to examine my personal accounts unless I am accused of a crime that requires that examination. And then a judge must order that examination.

Comment Submitted by Chris McKittrick

**Comment**

View document:

A terrible and wasteful idea.

Comment Submitted by Carol Rolf

**Comment**

View document:

Really? As if you don't invade our privacy enough anyway you need to resort to social media because you're not getting enough of what you want? And if I have an opinion about something it could possibly trigger your scrutiny? Well, I for one will not be bullied into paranoia that you might be watching and wasting taxpayers money. This is not the American way and this needs to stop.

Comment Submitted by Luke Stirling

**Comment**

View document:



I already make it a point to avoid travel to or through the US as it is because it's invasive and unpleasant, and I last did so over a decade ago. I can scarcely believe the steps taken since then and what is proposed in the future.

Comment Submitted by Emma Llanso

The full comments of the Center for Democracy & Technology are attached. In brief, CDT is deeply concerned that this proposal would invade the privacy and chill the freedom of expression of visitors to the United States and United States citizens.

Under the proposed changes, visitors to the U.S. who seek admittance through the Electronic System of Travel Authorization (ESTA), or complete Form I-94W, will be subject to unspecified review and monitoring of their public online activity by U.S. Customs and Border Protection (CBP) officials. This program will also increase the surveillance of U.S. citizens, both as a result of their online connections to visitors to the U.S. and because other countries may seek similar information from U.S. citizens traveling abroad. The burdens of this scrutiny will undoubtedly fall disproportionately on visitors and U.S. citizens who are Muslim or who have connections to the Middle East.

In addition to these challenges for fundamental rights, the proposal has a number of practical drawbacks as well. First, it is unlikely to yield useful information for CBP officials. Bad actors could easily circumvent the request by providing intentionally false or incomplete information. Further, the expense of the proposed data collection and analysis is significantly underestimated in the Request for Comment. In-depth, unbiased evaluation of a prospective visitor's public social media posts and connections cannot be accomplished in an automated fashion and would require extensive and costly human review.

For all of these reasons, we urge DHS to withdraw this proposal and to reject any approach that involves suspicionless monitoring and review of individuals' social media activity.

1401 K Street NW, Suite 200, Washington, DC 20005

**Comments of the Center for Democracy & Technology**

***Regarding Agency Information Collection Activities: Arrival and Departure Record***

***(Forms I-94 and I-94W) and Electronic System for Travel Authorization***

*19 August 2016*

The Center for Democracy & Technology appreciates the opportunity to provide comments to the Department of Homeland Security on its proposal to begin requesting disclosure of social media identifiers and other online account information from Visa Waiver Program applicants. DHS proposes to ask foreign visitors applying for a waiver of visa requirements to provide "information associated

with [their] online presence,” including the “provider/platform” and “social media identifier” used by the applicant. While the details of this proposed information collection are unclear, DHS’s Notice of Collection Activities states that the solicited online identity information “will enhance the existing investigative process” and “provide DHS greater clarity and visibility to possible nefarious activity and connections” of visitors to the United States.<sup>1</sup>

CDT is deeply concerned that this proposal would invade the privacy and chill the freedom of expression of visitors to the United States and United States citizens.

Under the proposed changes, visitors to the U.S. who seek admittance through the Electronic System of Travel Authorization (ESTA), or complete Form I-94W, will be subject to unspecified review and monitoring of their public online activity by U.S. Customs and Border Protection (CBP) officials. This program will also increase the surveillance of U.S. citizens, both as a result of their online connections to visitors to the U.S. and because other countries may seek similar information from U.S. citizens traveling abroad. The burdens of this scrutiny will undoubtedly fall disproportionately on visitors and U.S. citizens who are Muslim or who have connections to the Middle East.

In addition to these challenges for fundamental rights, the proposal has a number of practical drawbacks as well. First, it is unlikely to yield useful information for CBP officials. Bad actors could easily circumvent the request by providing intentionally false or incomplete information. Further, the expense of the proposed data collection and analysis is significantly underestimated in the Request for Comment. In-depth, unbiased evaluation of a prospective visitor’s public social media posts and connections cannot be accomplished in an automated fashion and would require extensive—and costly—human review.

For all of these reasons, we urge DHS to withdraw this proposal and to reject any approach that involves suspicionless monitoring and review of individuals’ social media activity.

1 U.S. Customs & Border Protection, Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and

Electronic System for Travel Authorization, FederalRegister.gov (June 23, 2016),

[https://www.federalregister.gov/articles/2016/06/23/2016-14848/agency-information-collection-activities-arrival-and-departure-recordforms-](https://www.federalregister.gov/articles/2016/06/23/2016-14848/agency-information-collection-activities-arrival-and-departure-recordforms-i-94-and-i-94w-and)

[i-94-and-i-94w-and](https://www.federalregister.gov/articles/2016/06/23/2016-14848/agency-information-collection-activities-arrival-and-departure-recordforms-i-94-and-i-94w-and) (hereinafter “Federal Register Notice”).

1401 K Street NW, Suite 200, Washington, DC 20005

**I. Requesting disclosure of online identifiers in the Customs process would create a significant burden on the free expression and privacy of international travelers.**

The proposed information collection would affect visitors who are traveling with a passport issued by one of the Visa Waiver Program designated countries, including Japan, South Korea, Singapore, Chile, Taiwan, and many members of the European Union and other European countries.<sup>2</sup> If arriving by air or sea, these travelers must fill out an ESTA form at least 3 days before their intended arrival to the U.S. and renew it at least every two years. In 2014, over 22 million visitors entered the U.S. through the Visa Waiver Program.<sup>3</sup> In addition to tourists, this includes family members, patients, amateur athletes and musicians, scholars, conference attendees, business visitors, and entrepreneurs.<sup>4</sup>

The scope of these visitors' online activity is enormous, and the proposal provides no definition of "online presence", "provider/platform", or "social media identifier" to narrow the field. This creates the potential for an overly broad or arbitrary interpretation by CBP officials or applicants who are concerned about being denied a visa waiver. Millions of websites and online services allow, and sometimes require, users to create a username or other identifier to post content and connect with other users. In the realm of travel-related services alone there are dozens of sites and apps that might fit the bill, including TripAdvisor, Yelp, AirBnB, VRBO, Couchsurfing, Hostelworld, Uber, Lyft, TripIt, Google+ (including Google Maps and Translate), Foursquare, and WikiTravel. Or DHS may be focused on more general-purpose services such as Facebook, Twitter, YouTube, SnapChat, Instagram, Pinterest, Tumblr, Reddit, LiveJournal, XING, StudiVZ, Hyves, Fotolog, KakaoTalk, LINE, WeChat, Pixnet, Xuite, Plurk, or even dating services such as Tinder, Grindr, and OKCupid. Any of these, and thousands more, could represent a portion of an individual's "online presence". DHS has provided no explanation of what type of response it expects from visitors.

While the Request for Comments describes the request for applicants' social media identifiers as "an optional data field," applicants for a visa-waiver will likely feel compelled to disclose significant amounts of personal information in response to this question. The majority of the data fields on the ESTA form are mandatory, and absent a specific indication to the contrary, it is likely that applicants will presume this question is mandatory as well.

<sup>2</sup> A full list of Visa Waiver Program designated countries is available at 8 C.F.R. § 217.2.

3 2014 Yearbook of Immigration Statistics, *available at*

[https://www.dhs.gov/sites/default/files/publications/table28d\\_7.xls](https://www.dhs.gov/sites/default/files/publications/table28d_7.xls). In 2010, Visa Waiver Program visitors

contributed over \$60 billion in tourism revenue. The White House, Office of the Press Secretary, Obama Administration Continues Efforts to Increase Travel and Tourism in the United States (May 10, 2012), *available at*

<https://www.whitehouse.gov/the-press-office/2012/05/10/obama-administration-continues-efforts-increase-travel-and-tourism-unite>.

The U.S. Travel Association estimates that, in 2015, Visa Waiver Program visitors “generated

\$120 billion in total output for the U.S. economy, supporting nearly 800,000 American jobs.” U.S. Travel Association, Visa Waiver Program, *available at* <https://www.ustravel.org/issues/visa-waiver-program>.

4 U.S. Department of State, Bureau of Consular Affairs, Visa Waiver Program, *available at*

<https://travel.state.gov/content/visas/en/visit/visa-waiver-program.html>.

1401 K Street NW, Suite 200, Washington, DC 20005

Even if this question is clearly marked “optional”, however, most applicants will likely feel substantial pressure to provide some information in response, because it is unclear whether refusing to provide this information could result in CBP officials drawing adverse inferences. The consequences of a visa waiver

denial to the visitor, her family, her business associates, and her fellow travelers can be

significant. Travelers are able to fill out an ESTA application online at their convenience. The form takes an average of 20 minutes and there is a \$14 fee per application.<sup>5</sup> In contrast, visa applications require the applicant to visit a consulate in person and can take months to process.<sup>6</sup> Assuming the traveler has enough time to apply for a visa after being denied a waiver, the B1 visa costs at least \$160, plus any expenses incurred traveling to a consulate to apply in person.<sup>7</sup> As a result, if a traveler’s ESTA application is rejected, that traveler could be prevented from coming to the U.S. entirely. This creates a considerable incentive to respond thoroughly to every question asked in the waiver-request process.

Potential visitors to the U.S. will thus be faced with a choice between two undesirable options: decline to disclose information about their online identity and risk being denied a waiver for providing incomplete information, or disclose this information and risk denial due to inaccurate or prejudicial

inferences made about their online activity. It is unclear what sort of online activity CBP officials would consider to merit denial of a visa waiver; as we discuss below, evaluation of public social media posts and connections for accurate, actionable intelligence is an extremely complex task. As a practical matter, applicants would have little or no opportunity to explain information associated with their online profiles or challenge inappropriate denial of a visa waiver. And, while denial of a person's visa waiver

request does not preclude their entry to the U.S. by a standard visa, most travelers would reasonably assume that an adverse decision on their ESTA application would translate to a similarly adverse decision on the issuance of a visa.

Thus, this proposal will create a chilling effect for travelers wishing to come to the U.S.<sup>8</sup> The risk of denial based on their online presence could lead some visa-waiver applicants to delete sensitive or controversial accounts in preparation for travel to the U.S., or simply to forgo an online presence at all. The strong incentives to disclose, and the unknown risks of nondisclosure, will compel many other applicants to share abundant information about their online activity. Most of these innocent disclosures will be useless for screening purposes, but they may still be used to augment the growing intelligence surveillance apparatus—with little legal protection for personal information and few, if any, mechanisms to safeguard against abuse.

5 Department of Homeland Security, Official ESTA Application, <https://esta.cbp.dhs.gov/esta/>.

6 Visas can take months to process. U.S. Customs & Border Protection, Frequently Asked Questions about the

Visa Waiver Program (VWP) and the Electronic System for Travel Authorization (ESTA),

<https://www.cbp.gov/travel/international-visitors/frequently-asked-questions-about-visa-waiver-program-vwp-and-electronic-system-travel>.

7 U.S. Bureau of Consular Affairs, Visitor Visa, <https://travel.state.gov/content/visas/en/visit/visitor.html#fees>.

8 See, e.g., Caution on Twitter urged as tourists barred from US, BBC.com (Mar. 8, 2012), <http://www.bbc.com/news/technology-16810312>.

1401 K Street NW, Suite 200, Washington, DC 20005

**II. The proposed collection is highly invasive and offers no assurances against abuse.**

Currently, the visa-waiver application solicits information about a prospective visitor's name, address, and citizenship, as well as topics such as their criminal background, health status, and whether they have overstayed a visa on a previous trip. While this information is certainly personal, the material associated with an individual's online presence can reveal a much deeper insight into a person's personality, preferences, ideas, and values. And the nature of social media technology in particular also exposes information about other people in their networks.

International travelers rely on social media and apps to find and purchase flights and accommodations, to find information about Customs procedures, to read and write travel reviews, to follow local news and make new connections, to communicate over long distances with colleagues, friends, and family back home, to contact their embassies or consular services in an emergency, and more. The DHS proposal would, in effect, ask travelers to give CBP a window into all of these online activities without clear standards for protecting those who disclose their online profiles and those in their networks. Moreover, travelers may not be fully aware of the entire scope of information that they are disclosing. Many internet users have multiple social media accounts, sometimes dating back a decade or more. Visitors may list these outdated accounts, forgetting they contain posts and connections that are out of date. And even if a person withholds particular identifiers that are associated with sensitive content (e.g., a Grindr profile) or connections (e.g., a controversial Facebook group), investigators may be able to unearth these accounts based on the information that is disclosed.

Further, accounts on some social media sites routinely display third-party posts and comments that were added to the account owner's page without her knowledge or consent. Depending on the user's privacy settings, some of these posts could be from complete strangers. Such posts may contain inaccurate or deliberately misleading information. Social media login credentials can also be compromised,

and accounts hijacked, to disseminate content that the person did not or would not post.<sup>9</sup>

A person's social media activity also necessarily reveals information about people in her social networks, including her family members, friends, and "followers"; therefore, disclosing a social media identifier to DHS could subject a person's close and distant associates to invasive scrutiny and exposure without their consent. This could create particular risks for journalists, lawyers, clergy, human rights workers, and others whose professions require confidentiality or who may face serious consequences

if their social media profile were taken out of context. The recent experiences of a Wall Street Journal reporter pressured to give CBP access to her mobile devices<sup>10</sup> and an Al Jazeera journalist discovering

9 See, e.g., Kate Conger, How activist DeRay Mckesson's Twitter account was hacked, Tech Crunch (June 10,

2016), <https://techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-account-was-hacked/>.

10 Joseph Cox, WSJ Reporter: Homeland Security Tried to Take My Phones at the Border, Vice Motherboard

(July 21, 2016), [http://motherboard.vice.com/en\\_uk/read/wsj-reporter-homeland-security-tried-to-take-my-phones-at-the-border](http://motherboard.vice.com/en_uk/read/wsj-reporter-homeland-security-tried-to-take-my-phones-at-the-border).

1401 K Street NW, Suite 200, Washington, DC 20005

he was placed on an NSA watch list<sup>11</sup> highlight the risks such surveillance programs pose to civil society institutions including the free press.

Social media posts are also vulnerable to interpretive error. The content and conversation on a person's page or feed is highly context-dependent, making it prone to misinterpretation—particularly when the interpreter does not speak the language or lacks cultural, colloquial, or idiosyncratic touchstones necessary for accurate understanding of the content. Similarly, metadata, including contacts within a person's list of "followers" or "follows," can be easily misconstrued when divorced from the context of the connection. Without the contextual understanding that a person is a journalist or human rights researcher, for instance, her connection to violent extremist accounts could appear suspect.<sup>12</sup> People collect many diverse social media connections, and may not even be aware of the identity behind an account that they follow. In fact, one study found that the *majority* of friendships on Facebook are not based on a "real", non-casual relationship.<sup>13</sup> These features undermine the value of this data and increase the risk of erroneous denial of a visitor's ESTA application.

Finally, the proposal does not protect applicants from the risk of improper conclusions based on declining to disclose "online presence" indicators. If DHS discovers the existence of an undeclared account, will the applicant be flagged for additional scrutiny? Will CBP officials draw negative inferences from the privacy settings an applicant has placed on his accounts? These questions remain unanswered. The proposal describes no recourse for individuals who believe they were improperly

denied a visa waiver, or subsequent visa application, based on their online presence.

**III. Collecting online identifiers from visitors to the U.S. would be a significant expansion of U.S. intelligence activity.**

This proposal seeks to implement an intelligence-gathering program in the form of a Customs administration mechanism, under the auspices of the Paperwork Reduction Act. Data collected through the I-94W and ESTA forms is not limited to determining an applicant's eligibility for a visa waiver. DHS engages in massive collection and analysis of open-source data<sup>14</sup> and has invested in

<sup>11</sup> Cora Currier, Glenn Greenwald, & Andrew Fishman, U.S. Government Designated Prominent Al Jazeera

Journalist as "Member of al Qaeda," Intercept (May 8, 2015),

<https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaedamember-put-watch-list/>.

<sup>12</sup> Human Rights Watch, With Liberty to Monitor All: How Large-Scale U.S. Surveillance is Harming Journalism,

Law and American Democracy, July 2014, *available at* [https://www.aclu.org/report/liberty-monitor-all-how-largescale-](https://www.aclu.org/report/liberty-monitor-all-how-largescale-us-surveillance-harming-journalism-law-and-american)

[us-surveillance-harming-journalism-law-and-american](https://www.aclu.org/report/liberty-monitor-all-how-largescale-us-surveillance-harming-journalism-law-and-american).

<sup>13</sup> R.I. Dunbar, Do online social media cut through the constraints that limit that limit the size of offline social

networks?, Royal Society: Open Science, January 2016, *available at*

<http://rsos.royalsocietypublishing.org/content/3/1/150292>.

<sup>14</sup> See Office of Inspector General, Dep't of Homeland Security, DHS Uses Social Media To Enhance Information

Sharing and Mission Operations, But Additional Oversight and Guidance Are Needed, No. OIG-13-115 (September 2013), *available at* [https://www.oig.dhs.gov/assets/Mgmt/2013/OIG\\_13-115\\_Sep13.pdf](https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-115_Sep13.pdf).

1401 K Street NW, Suite 200, Washington, DC 20005

systems of automated social media analysis.<sup>15</sup> Increased collection and retention increases the risk of data breach, as well as the potential for misuse and abuse. Harassment and fraud are among the biggest risks to users and institutions, such as banks or hospitals, when social media identifiers are breached.<sup>16</sup>



Further, all of the information collected through the visa-waiver program is shared, in bulk, with U.S. intelligence agencies and will be used to seed more intelligence surveillance unrelated to the applicant's eligibility for a visa waiver.<sup>17</sup> If this proposal is adopted, social media identifiers – tied to the true identity of visa-waiver applicants – will be shared with the National Security Agency which can then use the information to target applicants for surveillance. Data collected under this proposal would feed into intelligence surveillance for much broader purposes and without meaningful controls. Once in the Intelligence Community (IC), elements of the IC can then use the information provided to pursue their missions. This data is likely to be used to augment existing lists and databases for tracking persons of interest to law enforcement and intelligence agencies, with consequences for innocent individuals swept up in those surveillance programs. And to the extent the applicant's social media account reveals those with whom the applicant communicates (see discussion above), those persons can be targeted as well.

Under current law, Visa Waiver Program travelers – by definition, non-U.S. persons outside the United States – who are affected by expanded surveillance under this proposal will have no recourse against abuse. Specifically, surveillance under Executive Order 12333 is conducted without any judicial oversight. It can be conducted to collect “foreign intelligence information,” which includes information about the “activities” of any non-American abroad. Collection of information about these broadly defined “activities” is permissible even if there is no reason to believe that those activities threaten U.S. national security, are relevant to U.S. foreign policy, or are conducted by a person who is an agent of foreign power. Likewise, surveillance under Section 702 of the Foreign Intelligence Surveillance Act proceeds without meaningful judicial authorization, for broadly defined purposes, and regardless of whether there is information indicating that the target of surveillance is a criminal, a threat, or an agent of a foreign power. As non-U.S. persons, prospective travelers have only limited Privacy Act

15 Ellen Nakashima, DHS monitoring of social media worries civil liberties advocate, Wash. Post (Jan. 13, 2013),

<https://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-libertiesadvocates/>

[2012/01/13/gIQANPO7wP\\_story.html](https://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-libertiesadvocates/2012/01/13/gIQANPO7wP_story.html).

16 Tracy Kitten, Social Media Plays Key Role in Bank Fraud, Data Breach Today (Aug. 3, 2016),

<http://www.databreachtoday.com/interviews/social-media-plays-key-role-in-bank-fraud-i-3277>.

17 See, e.g., Department of Homeland Security, Privacy Impact Assessment Update Electronic System for Travel

Authorization (ESTA), DHS/CBP/PIA-007(f), June 20, 2016, at 5, *available at*

[https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-june2016\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-june2016_0.pdf) (“CBP will continue to

share ESTA information in bulk with other federal Intelligence Community partners (e.g., the National Counterterrorism Center), and CBP may share ESTA on a case-by-case basis to appropriate state, local, tribal,

territorial, or international government agencies.”).

1401 K Street NW, Suite 200, Washington, DC 20005

protections under the Judicial Redress Act, and these do not provide a guarantee against intelligence surveillance that targets an individual’s expressive activity.

The community impacts of this proposal will go far beyond the denial of an individual traveler’s visawaiver

application. Data collection and data sharing within the government imposes serious privacy costs that fall disproportionately on certain groups.<sup>18</sup> Social networks, in particular, lend themselves to association fallacies that can impact entire communities. Persons who are, or are presumed to be, of Muslim faith or Arab descent already face a disproportionate risk of religious and ethnic profiling while traveling, including enhanced TSA screening measures, wrongful inclusion on national security watchlists, and discriminatory citizen complaints.<sup>19</sup> Including travelers’ usernames, posts, and social media affiliations in the screening process will increase the dangers of “flying while Muslim,” particularly where cultural and linguistic barriers create an elevated risk of misunderstanding. A traveler who is wrongfully denied a visa waiver because of a distinct Arabic name or theological posts will suffer unfair and unjustified travel delays. And, in the process, her social media friends and followers will also be swept up in social media profiling. To the extent that the traveler’s social network overlaps with her religious and ethnic community, those individuals will also be exposed to increased scrutiny and its consequences for safety and privacy.

**IV. Americans will be swept up in social media collection and surveillance activities at home, and will face reciprocal disclosures requirements abroad.**

If this proposal is adopted, it will disproportionately affect Arab-Americans and Muslim Americans whose family members, guests, colleagues, and business associates are flagged or denied a visa waiver as a result of their online presence. Moreover, DHS – and, by extension, the rest of the Intelligence Community – will necessarily acquire information about Americans whose accounts are affiliated with those scrutinized and flagged profiles.

This proposal would create significant risks of ideological profiling, if travelers are subjected to elevated scrutiny merely because they have expressed a strongly-held religious or political belief

18 See, e.g., Alvaro M. Bedoya, *The Color of Surveillance*, *Slate* (Jan. 18, 2016),

[http://www.slate.com/articles/technology/future\\_tense/2016/01/what\\_the\\_fbi\\_s\\_surveillance\\_of\\_martin\\_luther\\_king\\_says\\_about\\_modern\\_spying.html](http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html).

19 American travelers have been plagued by profiling based on skin color, language, attire, and other markers of

religious and ethnic background. See, e.g., Catherine Rampell, *Ivy League economist ethnically profiled, interrogated for doing math on American Airlines flight*, *Wash. Post* (May 7, 2016),

[https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doingmath-](https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doingmath-on-american-airlines-flight/?tid=a_inl&utm_term=.00e58cfbfc37)

[on-american-airlines-flight/?tid=a\\_inl&utm\\_term=.00e58cfbfc37](https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doingmath-on-american-airlines-flight/?tid=a_inl&utm_term=.00e58cfbfc37); Peter Holley, *Muslim couple says they were*

kicked off Delta flight for using phone, saying ‘Allah,’ *Wash. Post* (Aug. 7, 2016),

[https://www.washingtonpost.com/news/morning-mix/wp/2016/08/07/muslim-couple-says-they-were-kicked-offdelta-](https://www.washingtonpost.com/news/morning-mix/wp/2016/08/07/muslim-couple-says-they-were-kicked-offdelta-flight-for-using-phone-saying-allah/?tid=a_inl)

[flight-for-using-phone-saying-allah/?tid=a\\_inl](https://www.washingtonpost.com/news/morning-mix/wp/2016/08/07/muslim-couple-says-they-were-kicked-offdelta-flight-for-using-phone-saying-allah/?tid=a_inl); Carma Hassan & Catherine E. Shoichet, *Arabic-speaking*

student kicked off Southwest flight, *CNN.com* (Apr. 8, 2016),

<http://www.cnn.com/2016/04/17/us/southwestmuslim-passenger-removed/>.

1401 K Street NW, Suite 200, Washington, DC 20005

online. Ideological exclusion of visitors would deny Americans access to information and opportunities for cultural and educational exchange that spur creativity and innovation. And American businesses would suffer economic impacts when foreign scholars, colleagues, and investors are delayed or denied entry. Potential visitors may decide instead to censor themselves online, rather than risk exclusion,

which would further diminish Americans' access to information and opportunity for informed debate. As a network, the value of the global internet is related to the size and engagement of its participants; withdrawal of certain groups or communities diminishes the value of a network for all members.<sup>20</sup> Finally, if this proposal is enacted, Americans will likely face reciprocal social media disclosure requirements when traveling abroad. Customs and immigration policy is notoriously susceptible to reciprocity effects, and the U.S. Visa Waiver Program is no exception. Currently, for example, the European Commission is considering restricting visa-free travel for Americans and Canadians in response to the absence of a visa-waiver path for nationals of some EU member states.<sup>21</sup> Americans traveling to Iran, Iraq, Syria, or Sudan could face higher hurdles, including social media disclosure requirements, in retaliation for the U.S. decision to exclude any recent travelers or dual nationals of those countries from eligibility for a visa waiver.<sup>22</sup> And all countries could be incentivized to implement online identity disclosures in the event that the U.S. expands its social media inquiry to visa applications.

For Americans traveling abroad, reciprocal social media disclosure requests could create travel delays and legal risk for speech that is protected under the United States Constitution. In non-visa waiver countries with fewer legal safeguards, disclosure requirements could expose American travelers to serious consequences such as border interrogations, administrative detentions, and other more serious penalties for social media activity that offends customs or norms against homosexuality, female immodesty, or religious or ideological dissent.<sup>23</sup> Other states' use of social media screening as an element of border security has demonstrated the significant risk of ideological and ethnic profiling that these programs create.<sup>24</sup> For example, in 2014, the U.S. Consulate in Jerusalem noted that "U.S. citizen visitors have been subjected to prolonged questioning and thorough searches by Israeli

<sup>20</sup> See Yochai Benckler, *Wealth of Networks: How Social Production Transforms Markets and Freedom* (2007).

<sup>21</sup> Tara Palmeri & Maïa de la Baume, *EU considers restricting visa-free travel for Americans, Canadians*, Politico

(Apr. 7, 2016), <http://www.politico.eu/article/eu-considers-restricting-visa-free-travel-for-americans-canadians/>.

The U.S. sets visa policy on a country-by-country basis; some EU members are not part of the U.S. Visa Waiver

Program. This has led the European Commission to re-examine its visa policies for the United States. *Id.*

22 Paul Dallison, U.S. visa changes hit Europeans, Politico (Jan. 22, 2016),  
[http://www.politico.eu/article/us-visachanges-](http://www.politico.eu/article/us-visachanges-hit-europeans-dual-nationality-iran-iraq-syria/)

[hit-europeans-dual-nationality-iran-iraq-syria/](http://www.politico.eu/article/us-visachanges-hit-europeans-dual-nationality-iran-iraq-syria/).

23 *See, e.g.*, the case of British national Stephen Comiskey, who was reportedly entrapped by Saudi police, jailed,

and sentenced to death for homosexuality before the United Kingdom managed to negotiate his release. Nick

Parker, Execution fear of gay Brit battered in Saudi, theSun.co.uk (Mar. 31, 2011),

<https://www.thesun.co.uk/archives/news/463707/execution-fear-of-gay-brit-battered-in-saudi/>.

Singapore, which

also criminalizes same-sex sexual relations, is a visa-waiver country.

24 Diaa Hadid & Joseph Federman, Israel asks Arab visitors to open emails to search, NBCNews.com (June 5,

2012), [http://www.nbcnews.com/id/47690140/ns/world\\_news-mideast\\_n\\_africa/t/israel-asks-arab-visitors-openemails-](http://www.nbcnews.com/id/47690140/ns/world_news-mideast_n_africa/t/israel-asks-arab-visitors-openemails-search/)

[search/](http://www.nbcnews.com/id/47690140/ns/world_news-mideast_n_africa/t/israel-asks-arab-visitors-openemails-search/).

1401 K Street NW, Suite 200, Washington, DC 20005

authorities upon entry or departure. Those whom Israeli authorities suspect of being of Arab, Middle Eastern, or Muslim origin [...] may face additional, often time-consuming, and probing questioning by immigration and border authorities, or may even be denied entry into Israel or the West Bank."<sup>25</sup> All Americans have an interest in ensuring that social media border-screening programs do not become an international norm.

## **V. Online identifier collection would be ineffective and will impose significant unaccounted costs.**

DHS indicates that collection of visa-waiver applicants' online identity information will "enhance the existing investigative process" for screening visa-waiver applicants.<sup>26</sup> DHS has previously argued that generally increasing ESTA data-collection will streamline the visa-waiver application process by reducing the number of false-positive matches between applications and terrorism watchlists.<sup>27</sup> These empirical arguments rest on several flawed assumptions.

First, the ease of circumvention undermines this program's utility. Individuals who pose a threat to the

United States are highly unlikely to volunteer online identifiers tied to information that would raise any question about their admissibility to the United States. Such questioning is far more likely to yield a flood of profiles from unsuspecting travelers who feel compelled to disclose information. It may also prompt some travelers to create false or “dummy” accounts to shield their privacy—or to deliberately undermine CBP agents’ investigations.

Second, sorting through the quantity of information included in an individual’s online presence creates a tremendous and costly administrative burden. Information traditionally collected as part of the visa process (names, birthdates, and place of birth, for example) includes single data points that can be easily cross-referenced against prepared indices such as watchlists or hotspots for terrorism or infectious diseases. By contrast, social media identifiers will yield messy and multidimensional data sets. As discussed above, social media in particular is vulnerable to misinformation and misinterpretation errors. Further, one identifier can expand the available data by many orders of magnitude with no comparable qualitative increase in information or intelligence. Given that the average internet user has five social media profiles,<sup>28</sup> this proposal would introduce significant noise and little if any discernable signal to the visa-waiver screening process.

25 U.S. Consulate in Jerusalem, Entering and Exiting Jerusalem, the West Bank, and Gaza,

<https://jru.usconsulate.gov/u-s-citizen-services/local-resources-of-u-s-citizens/entering-exiting/>; see also Adam

Taylor, These accounts from Arab Americans show why an Israeli visa waiver plan is so controversial, Wash.

Post (Apr. 27, 2014), [https://www.washingtonpost.com/news/worldviews/wp/2014/04/27/these-](https://www.washingtonpost.com/news/worldviews/wp/2014/04/27/these-accounts-from-arab-)

[accounts-from-arab-](https://www.washingtonpost.com/news/worldviews/wp/2014/04/27/these-accounts-from-arab-americans-show-why-an-israeli-visa-waiver-plan-is-so-controversial/)

[americans-show-why-an-israeli-visa-waiver-plan-is-so-controversial/](https://www.washingtonpost.com/news/worldviews/wp/2014/04/27/these-accounts-from-arab-americans-show-why-an-israeli-visa-waiver-plan-is-so-controversial/) .

26 Federal Register Notice, *supra* n.1.

27 U.S. Customs & Border Protection, Strengthening Security of the VWP through Enhancements to ESTA,

<https://www.cbp.gov/travel/international-visitors/esta/enhancements-to-esta-faqs>.

28 Jason Mander, Internet users have average of 5.54 social media accounts, GlobalWebIndex.net (Jan 23,

2015), <http://www.globalwebindex.net/blog/internet-users-have-average-of-5-social-media-accounts>. The average

1401 K Street NW, Suite 200, Washington, DC 20005

Third, transforming raw social media data into actionable intelligence will require new capabilities in machine learning and complex network analytics—increasing costs and introducing new sources of error into the screening process. There may be useful data points that could produce insights or investigative leads amid the deluge of irrelevant and potentially false information gathered in response to this question. But, given the complexity of the dataset, CBP officers cannot conduct a cursory analysis. Even in combination with simple algorithmic screening against prepared databases and indices, this type of analysis is minimally accurate. Currently, machine learning used to identify jihadist accounts on Twitter exhibits an error rate of 10 to 24 percent.<sup>29</sup> Such an error rate would represent between 2 and 5 million annual visitors being falsely flagged under the Visa Waiver Program.<sup>30</sup> And because these algorithms are biased against foreign languages, particularly those not based on the Roman alphabet, the error rate for algorithmic assessment of social media information collected under this proposal will likely be even higher. By using unreliable and misleading social media activity as a proxy for admissibility, DHS will experience an increase in incidence of false-positive error.<sup>31</sup>

Moreover, machine learning can also introduce false negatives into a risk assessment. For example, if an algorithm is trained to identify whether an applicant is a person of interest, a positive match between an applicant's name and biographical information and an identity on a terrorism watchlist will result in a red flag. However, when social media information is added to the evaluation, there is a risk that it can contradict or discredit a database match, removing a correctly identified red flag from the application.<sup>32</sup> Given that machine learning processes introduce serious risks of both false-positive and false-negative signals, the necessity of human review cannot be avoided.

The more deeply a CBP investigator delves into an applicant's social media profile, however, the more training and context she will need in order to overcome the interpretive errors inherent in social media content and connection analysis. Some of the best technology in use today for identifying ISIS accounts social media user posts frequently and has the ability to post various types of data. A majority of Facebook,

Instagram, and Twitter users post at least once per week. Maeve Duggan et. al, Frequency of Social Media Use,

Pew Research Center (Jan 9, 2015), <http://www.pewinternet.org/2015/01/09/frequency-of-social-media-use-2/>.

29 Enghin Omer, Thesis: Using machine learning to identify jihadist messages on Twitter, Uppsala University,

Sweden, July 2015, <http://uu.diva-portal.org/smash/get/diva2:846343/FULLTEXT01.pdf>.

30 2014 Yearbook of Immigration Statistics, *available at*

[https://www.dhs.gov/sites/default/files/publications/table28d\\_7.xls](https://www.dhs.gov/sites/default/files/publications/table28d_7.xls).

31 Sarah Foxen & Sarah Bunn, Forensic Language Analysis, 509 POSTnote (Sept. 2015),

<http://www.forensiclinguistics.net/POST-PN-0509.pdf>.

32 This effect is a byproduct of algorithmic decisionmaking: Risk-assessment algorithms rely on various qualifying

criteria to determine whether an entry can be identified as “suspicious.” If the various fields of data pertaining to

an entry reinforce each other, this can increase the algorithm’s accuracy. But if these fields do not reinforce each

other and the standards for evaluating the contradictory information (for example, innocuous social media posts)

are not clearly delineated in the algorithmic rule, then it can reduce the accuracy of the algorithm by introducing

false-negative error in the “suspicion” assessment.

1401 K Street NW, Suite 200, Washington, DC 20005

includes automated analysis and human review and has a margin of error at 2.54 percent.<sup>33</sup> While this may first appear to be trivial, in practical effect it would mean nearly half a million visitors to the U.S. were denied a visa waiver, subject to significant additional scrutiny, and potentially deterred from visiting the U.S. every year. The combined effect of more error and more human review will result in substantial additional labor costs, which are not reflected in the DHS’s estimated cost to the public of \$265 million for the ESTA program proposal.<sup>34</sup>

\* \* \*

DHS’s proposal to collect the online identifiers of travelers under the Visa Waiver Program is highly invasive and will chill free expression online, will disproportionately affect Muslim and Arab communities within and outside the U.S., will lead to reciprocal burdens for Americans travelling abroad, and will be ineffective and prohibitively expensive. We urge DHS to withdraw the proposal. Respectfully submitted,



Nuala O'Connor

Emma Llansó

Rita Cant

Greg Nojeim

Michelle de Mooy

Joseph Lorenzo Hall

Aislinn Klos

Apratim Vidyarthi

Center for Democracy & Technology

33 J.M. Berger & Jonathon Morgan, The ISIS Twitter Census: Defining and describing the population of ISIS

supporters on Twitter 46, Brookings Inst., March 2015,

[http://www.brookings.edu/~media/research/files/papers/2015/03/isis-twitter-census-bergermorgan/isis\\_twitter\\_census\\_berger\\_morgan.pdf](http://www.brookings.edu/~media/research/files/papers/2015/03/isis-twitter-census-bergermorgan/isis_twitter_census_berger_morgan.pdf).

34 See Federal Register Notice, *supra* n.1. Under the Paperwork Reduction Act, annual cost burden estimates do

not include labor cost for the estimated burden-hours for a proposal. U.S. Office of Personnel and Management,

Paperwork Reduction Act Guide 2.0, 39, OPM.gov (April 2011), *available at* <https://www.opm.gov/about-us/opengovernment/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf>.

Comment Submitted by Anne Marshall

**Comment**

View document:

Not only unreasonable invasion of privacy, but an unreasonable financial and personnel burden on government services.

Comment Submitted by Charles Trebes

**Comment**

View document:

These overt steps on the way to a sophisticated digital Police State must stop and be reversed.

Comment Submitted by David Scott

**Comment**

View document:

You don't have to censor if you can make people afraid to speak to begin with. You don't have to exclude travelers if you can make them not want to come to our country and enjoy it.

Comment Submitted by Dorothy Newkirk

**Comment**

View document:

It is a bad idea and none of their business. Taking away freedoms supposedly to make us more secure does not make us more secure it doesn't do anything but take our freedoms away. 'Those who surrender freedom for security will not have, nor do they deserve, either one.'

- Benjamin Franklin

Comment Submitted by Faiza Patel, Brennan Center for Justice at NYU School of Law

**Comment**

View document:

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. As described in the document attached to this submission, 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.

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).

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.

<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).

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 –

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?

2 *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>.

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

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>

3 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).

4 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.”).

5 See Ye Hee Lee, *supra* note 3.

6 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>.

7 See, e.g., *Counterterrorism, Counterintelligence, and the Challenges of ‘Going Dark’: Hearing Before the S. Select Comm. on Intelligence*, 114th 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.*, 114th 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.”).

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

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>

4

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”?

9 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).

10 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>.

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

12 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.”).

13 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>.

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

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

5

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>

15 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/>.

16 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).

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).

6

Sincerely,

Faiza Patel

Co-Director, Liberty and National Security Program

Rachel Levinson-Waldman

Senior Counsel, Liberty and National Security Program



**Comment**

View document:

Dear sir or madame, this is a rather good example of unnecessarily invading peoples privacy while wasting time and resources at the same time. If an actual threat to your country would be dumb enough to actually post on his/hers social media anything truly noteworthy, they are clearly stupid enough to get caught without this kind of invasion of privacy to hundreds of millions of people every year. I'm rather confident that you (CIA, NSA etc...) already have enough algorhythmes going through the social media 24/7 to stop the truly dangerous individuals.

Comment Submitted by Brian Stanley

**Comment**

View document:

This proposal is wasteful, unlawful, and unconstitutional. It is a violation of the 14th Amendment, which states that everyone, aliens included, is guaranteed equal protection under the law. No one should be subject to such a gross violation of privacy.

Comment Submitted by Jernej Slapar

**Comment**

View document:

As a guy that grew up on the internets - this is just stupid - social accounts can be faked and the potential bad guy can seem like a really nice guy that no one would doubt. Simple facts are:

- \* real bad guys do not communicate in the open
- \* real bad guys will present a pleasant facade
- \* this proposition is just a security theatre that will make no one safer

Comment Submitted by Marie- Jeanne Leduc

**Comment**

View document:

i will never ever travel there

Comment Submitted by Joycelyn Maguire

**Comment**

View document:

This is a complete invasion of privacy. I protect who sees my information on my social media sites so that I can share opinions and ideas with my friends only as well as letting them see my family activities. This plan puts someone watching over my shoulder at every opportunity - next you will send spies to our tailgates!

Comment Submitted by Daniel Weiss

**Comment**

View document:

Investigations are only for criminal activity. Entering the country is not a criminal action, so no investigation should be needed. In America, we are innocent until proven guilty. Checking social media accounts is invasive and treats every person like a criminal suspect.

Comment Submitted by Bill Lindner

**Comment**

View document:

IT VIOLATES YOUR PRIVACY AND UNLESS YOU ACTUALLY ARE A CRIMINAL AND THERE IS EVIDENCE THAT YOU PLAN TO CAUSE HARM, YOU AND YOUR DATA SHOULD BE LEFT ALONE.

Comment Submitted by Simon Keldermans

**Comment**

View document:

This is an invasion of privacy.

Comment Submitted by Molly Widstrom

**Comment**

View document:

It is a gigantic invasion of privacy.

Comment Submitted by Jack Schwartz

**Comment**

View document:

unless the person has already been identifies as being guilty of a crime then HS has no right to ask or demand to know your on-line presence.

Comment Submitted by N N

**Comment**

View document:

This will not deter or stop anything. This is a breech of civil liberties.

Comment Submitted by Nathan White, Access Now

**Comment**

View document:

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

Re: Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization, Docket No. 2016-14848

We write to submit comments on the U.S. Department of Homeland Security (DHS) Customs and Border Protection (CBP)'s proposed changes to the Electronic System for Travel Authorization (ESTA) and Form I-94W, which would ask respondents to "enter information associated with [their] online presenceProvider/PlatformSocial media identifier." By asking travelers to provide the government with social media identifiers that could then be used to monitor online activity, the proposal risks undermining the rights to freedom of expression, freedom of association, and privacy. The CBP should withdraw the proposed rule change.

Access Now defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. As part of this mission, we fight for the right to speak freely, which is critical for demonstrating dissent, guaranteeing a free press, and defending human rights.

Following the publication of the request for comment, Access Now issued a survey requesting public responses to the proposed changes. More than 2,300 individuals responded to our survey. The overwhelming majority of respondents saw the proposal as negative. One respondent explained, "I

believe that requesting this information would have a chilling effect on free and open discussion on social media -- discussion that is essential to democracy." Another worried, "I am terrified that a meta-annalists [sic] of my past years search history (often helping or showing students how to search for topics due on term papers -- on both the computers at my college, and my personal ones as well) would yield a very skewed view of who I am or what I believe." Several respondents called CBP's proposal an invasion of privacy.

U.S. law guarantees the rights to freedom of expression, freedom of association, and privacy as provided for in the U.S. Constitution as well as the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights. Efforts to monitor social media activity have been shown to have a chilling effect on speech. Government monitoring and analysis of social media content, even public content, can reveal a significant amount of non-public, protected information about a user and thus interfere with the right to privacy.

Surveillance of this sort has a disparate impact on users at risk, including communities of color, religious groups, LGBTQI communities, and other marginalized communities. As one respondent noted, this proposal "might bring a lot of harm when it is politically abused." The internet has become a space for vulnerable communities to connect with one another. Social media surveillance is especially harmful to individuals living under repressive regimes where such expressions may be unlawful and subject to harsh penalties.

In addition, there is a high likelihood of confusion as to the purpose of CBP's collection and how the agency will use the data. For example, it is not immediately clear to what extent providing identifiers will impact decisions to grant immigration status to individuals entering the U.S. According to DHS, the ESTA "determines the eligibility of visitors to travel to the United States under the Visa Waiver Program (VWP)." CBP determines admissibility into the U.S. upon arrival, and no information has been provided about how the social media identifiers will impact this determination. It is also unclear whether, how, or to what extent user data will be used by other government offices and agencies.

The stated goals of the proposed rule changes are to "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." Yet, the activity and communications of people willing to provide social media identifiers to DHS are least likely to be of interest because individuals whose data DHS and other intelligence agencies seek would be unlikely to provide identifiers. Complicating matters further, large-scale analysis of social media implicit in the proposal is of questionable value due to the highly-contextual nature of expression on social media. As such, the proposal does not meet international human rights standards as articulated by the United Nations Human Rights Committee.

Attached, we provide additional data and the complete responses of the more than 2,300 survey participants.

Note: See this link for a 97 page attachment that includes 2300 survey responses: <https://www.regulations.gov/document?D=USCBP-2007-0102-0589>

Comment Submitted by Tony S

**Comment**

View document:

This is absurd long before since Carnivore you have unconstitutionally been stealing our PII. The good news is most are beginning to get tired of it. Fearmongering is not as effective as it once was.

Comment Submitted by Daemon Singer

**Comment**

View document:

We thinking folks, cannot understand why anyone would want to go to the United States of America. The USA is filled with people who don't realise there is a whole world out there, past their borders where not everyone has or feels a need to own a gun. This is because most Americans are either RWNJ christians, or simply US-trained micro-brains, not much good for anything at all outside their own borders.

I don't believe most Americans should be allowed to visit Australia based on their incredibly small IQ's as a nation.

Comment Submitted by Harold Watson

**Comment**

View document:

No! The Constitution expressly forbids such intrusions.

Comment Submitted by Gabriel Lica

**Comment**

View document:

Congratulations...finally some tough rules are to be implemented, protecting innocent people against the terrorists and criminals.

**Comments on the Customs and Border Protection Bureau (USCBP) Notice: [Agency Information Collection Activities: Arrival and Departure Record \(Forms I-94 and I-94W\) and Electronic System for Travel Authorization](#)**

Pages 9-16

---

Comment Submitted by Emma Llanso, Center for Democracy & Technology

Comment

View document:

Attached is a joint letter from 28 human rights and civil liberties organizations, expressing our deep concerns with the proposal from Customs and Border Protection to collect information about travelers' "online presence".

While we understand the security concerns that motivate this proposal, we believe it would irresponsibly shift government resources to a costly and ineffective program while invading the privacy of not just visa-waiver applicants, but also their contacts in the U.S. The price of a business trip or family vacation to the United States should not include a fishing expedition into one's reading lists, tastes, beliefs, and idiosyncrasies by CBP officers. Given the risk of discriminatory impact on minority communities as well as the privacy concerns set forth above, we urge CBP to withdraw this proposal.

Signed,

Access Now

Advocacy for Principled Action in Government

American Civil Liberties Union

American Immigration Lawyers Association

American-Arab Anti-Discrimination Committee

Americans for Immigrant Justice

Asian Americans Advancing Justice - AAJC

Bill of Rights Defense Committee/Defending Dissent Foundation

Coalition for Humane Immigrant Rights of Los Angeles

Center for Democracy & Technology

Committee to Protect Journalists

The Constitution Project

Consumer Action

Consumer Federation of America

Council on American-Islamic Relations

Demand Progress

Electronic Frontier Foundation

Illinois Coalition for Immigrant and Refugee Rights  
Immigrant Legal Resource Center  
National Coalition Against Censorship  
National Immigrant Justice Center  
National Immigration Project of the National Lawyers Guild  
New America's Open Technology Institute  
Online Policy Group  
Paradigm Initiative Nigeria  
Restore The Fourth  
TechFreedom  
Woodhull Foundation

---

Comment Submitted by Brooke Rusert

Comment

View document:

Invasion of privacy, absolutly unnecessary and a complete waste of money

---

Comment Submitted by L D Lloyd

Comment

View document:

I know I'm swimming up stream here... I notice that no one likes this proposal but no one offers an alternative solution. We are living in an era of US history where we all are going to have to make sacrifice for the safety of our citizens, our children and ourselves. Yes, it might be a pain for those trying to enter the US but how much inconvenience will one more question add to the stack of forms already required. Especially when the result would be greater security for you. I wonder what someone who has lost someone they loved to alien automatic weapons, bombs or machete's thinks about this proposal? We're talking about changes to save our lives and our country. Other countries go with stricter regulations than this proposal for the same reason. It seems the proposal is talking about aliens attempting to enter our country, not US citizens. Even after reading all of the comments here, I do not see anything unconstitutional in the proposal it's self. I see a lot of angry people, angry at the wrong things, reading into the proposal things that are not there. Nor intended to be there nor placed between the lines. This may not work but we need to find out if it will. Do you want your mother mowed down the next time she goes to the mall? Don't say it can't happen. Will this proposal PREVENT that? Probably not but it might help save someone. We've got to start somewhere. We've got to start soon. What suggestions,

short of arming everyone, do you have? A lot of people are listening. Here's your chance. What's YOUR proposal?

---

Comment Submitted by Courtney Bolton

Comment

View document:

I think it is a horrific invasion of privacy, and quite frankly, is none of their business.

---

Comment Submitted by Edith Borie

Comment

View document:

Here I am unsure, because I never use any social media, and have nearly zero online presence.

---

Comment Submitted by Michael Bay

Comment

View document:

I do NOT think they should have the right to look through my, or anyone's, social media to see if they are allowed into the United States.

---

Comment Submitted by Barbara Cohn

Comment

View document:

This is outrageous and it is none of their business.

---



Comment Submitted by Anna Clark

Comment

View document:

I think it's a ridiculous invasion of privacy, unless your profile is searchable by the public in general.

---

Comment Submitted by Anonymous

Comment

View document:

It violates my privacy

---

Comment Submitted by Charlene Boydston

Comment

View document:

Understand DHS is looking for terrorists! That being said, where do we draw the line for invasion of privacy? Or, do we now, no longer have that right? Personally, I have no problem with people reading my posts, if they don't like what I say, they can move on! I call it as I see it, but am not, nor have I ever been, a HOT head, a bully or terrorist!

---

Comment Submitted by LaDene Bean

Comment

View document:

Gross violation of my rights. Investigate the fraud and election tampering by the Clinton campaign if you need something positive to do.

---

Comment Submitted by William Colwell 3rd

Comment

[View document:](#)

These fishing expeditions DO NOT yield results. The continued push by government institutions to gather all on-line content is intrusive & ineffective. All it supports is identity theft and abuse by those with access to the data.

---

Comment Submitted by Lauren Clifford

Comment

[View document:](#)

I am not a reporter. I don't want my thoughts and ideas shared with social network friends analyzed by government officials. That's where I play.

---

Comment Submitted by Mandy Fox

Comment

[View document:](#)

This is another absurd plan to remove privacy under a cloak of security.

---

Comment Submitted by Hannah Banks

Comment

[View document:](#)

This is an unnecessary intrusion into our private stuff. Please don't do it.

Thanks for listening.

---

Comment Submitted by Kara Guatto

Comment

View document:

It's absolutely ridiculous and a complete invasion of privacy.

-----

Comment Submitted by Aaron Honore

Comment

View document:

RIDICULOUS!

-----

Comment Submitted by Ronald Hammersley

Comment

View document:

I assert my constitutional right to privacy.

-----

Comment Submitted by Dominick Falzone

Comment

View document:

The government should not search the intellectual content of electronic devises unless they have probable cause to believe that there is evidence of a crime.

-----

Comment Submitted by Barbara Garcia

Comment

View document:

Despicable

---

Comment Submitted by Kevin Breidenbach

Comment

View document:

I think it sounds like the stuff of a totalitarian surveillance state.

---

Comment Submitted by Rhiannon Beattie

Comment

View document:

Absolutely ridiculous. Would they also like to know what I have earned in the last year/decade and how I have spent it? I also suspect that the way the general public would be treated would be different to those with money and/or status

---

Comment Submitted by Mihail Comanescu

Comment

View document:

This is a direct attack on the constitution and even on basic human rights. I am not a criminal and therefore should not be presumed one by default. What I do on the internet is none of your damn business. It's enough that you know my passport and all information tied to it via interpol/IRS/DOJ, where I travel, which again shouldn't be the case, how much money and valuables I possess and scanned by the TSA. Enough is enough ! This is not 1984!

---

Comment Submitted by Gabriel Craciun

Comment

View document:

Not my country or my money, but wouldn't it be better spent building hospitals?

---

Comment Submitted by Emelie Grundberg

Comment

View document:

Should this happen, I doubt even half of the people who travel to America today will do so later. Many of our social networks are safe spaces, and even the thought of having a government scrutinize them for either 'real' or 'imagined' threats will probably affect a lot of people's future plans to visit the country.

Also, couldn't you find something much more useful to use your tax payers money for? Schools always need more funding, the salary of all those people working on a government pay could be raised - even if just by a little. You could spend it on research, on paving roads, on repairing buildings... So many other - better - things to spend billions of dollars.

I advise you to rethink this idea of yours. It'll only lead to more problems than you'll solve.

-----

Comment Submitted by Charles Collins

Comment

View document:

Although a right to privacy is not written into the constitution, it is understood to be essential to our representative democracy. I would rather accept the risk of living in a sometimes violent and unpredictable world than risk the further loss of this unwritten right.

-----

Comment Submitted by Margaret Goodman

Comment

I don't want Big Brother watching me.

-----

Comment Submitted by K. Arnone

Comment

Nineteen Eighty Four by Orwell was not a how to guide, but a warning. Stop living up to it's worst expectations.

-----

Comment Submitted by Roslyn Doctorow

Comment

View document:

absolutely not - I have a right to privacy

---

Comment Submitted by Pedro Freire

Comment

The private details of my 'online presence' should only be made available to any agency under a court order.

---

Comment Submitted by Holly Hartmann

Comment

The Department of Homeland Security should not be able to search my online presence every time I enter the country. This is Orwellian. It should not be allowed. Hoovering up all social media activity without probable cause or even a reasonable suspicion is not how a free democracy works. And collecting all the straws in a haystack does not protect us. Increase the trust of the people in law enforcement and provide for easy access to preventive mental health care. That will protect us. And national security doesn't mean too much to people in the US that lack economic or health security. Spend the \$300 Million dollars on that kind of security!

---

Comment Submitted by Carolyn DeVoe

Comment

I THINK THE ONLY ONES THEY SHOULD HAVE ACCESS TO, IS GOVERNMENT OFFICIALS, OR ANYONE WHO WORKS FOR GOVERNMENT JOBS, CITY STATE, COUNTRY..

---

Comment Submitted by Aubrey Barnard

Comment

Information on social media is largely irrelevant to national security and should not be part of any screening or customs process.

---

Comment Submitted by Debbie Evans

Comment

[View document:](#)

Overly intrusive and unnecessary. Would put me off visiting as feel prohibitive and invasion of my privacy.

---

Comment Submitted by Hannah Foster

Comment

[View document:](#)

Homeland security should be about providing for the prosperity and access to resources for individuals, not about banning and restricting people we don't agree with. The criteria used for determining whether social media content indicates someone is a threat, and even the criteria of determining what threats are is so arbitrary as to be unpolicable and unable to be properly transparent. Taxpayer money should be used for increasing socio-economic mobility, not taking it away. This level of surveillance would be tantamount to a step towards a fascistic governing body, and that goes against what we know to be the most prosperous form of governance for the greatest number of people.

---

Comment Submitted by Bill Gustavson

Comment

[View document:](#)

I strongly disagree with the idea of searching our online accounts, and think it is a slippery slope towards Big Brother checking everything people do online. It would also pave the way for censorship bills such as SOPA.

---

Comment Submitted by Calvin Howes

Comment

[View document:](#)

It won't work, it will be extremely invasive and expensive, and it will get hacked and leaked.

---

Comment Submitted by Susan Harman

Comment

View document:

DHS shouldn't exist.

---

Comment Submitted by Gage Bush

Comment

View document:

Remember this simple acronym!

D.

O.

N.

T.

DON'T!

---

Comment Submitted by Leslie Feuille

Comment

View document:

It is a massive invasion of privacy and a waste of taxpayer money.

---

Comment Submitted by Marjorie Glasscock

Comment

View document:



I do not do all that social media junk. I live in the real world with flesh-and-blood people. So I guess I'd be held at the border, huh? What an embarrassment we are becoming.

---

Comment Submitted by Jessica Dheere

Comment

View document:

This is a broad, disproportionate, and invasive approach that will not only be ineffective but will also further burden the customs and border protection. It will also have a negative effect on free expression in general and the already declining reputation of the United States in the world. This proposal is incredibly ignorant of international human rights and free speech norms but also the diversity of the global population and their opinions and the idea that opinions are not an indicator of anything except that the person has an opinion. It is highly unlikely that this practice will increase travelers' safety or security. Meanwhile, the potential for mistakes and misuse of such a program--given the stories we've already heard about CBP invading people's bodies and physical privacy--is unacceptably high. Focus your resources more narrowly, and legally, with justified warrants, and you might actually have more impact.

---

Comment Submitted by E Broadbent

Comment

View document:

Just because there is data out there to search, does not mean it is a good idea to do so. This removes the focus from traditional and proven methods, and builds distrust for the government, which ultimately is a much more serious threat to national security. When people believe in the integrity of their government and what it stands for, they readily support and defend it, instead of worrying about how intrusive it is or could be. Please rethink the entire practice and ambitions for gathering personal data on everyone, and instead focus on gathering intelligence on known sources of trouble and threats that can be discerned from suspicious purchase transactions, illegal and damaging acts, and the knowledge of people around the world who care for and work for the betterment of their societies. By building stronger relationships with people, not data, we can fight sources of terror and crime much more effectively. Thank-you.

---

Comment Submitted by Elaine Becker

Comment

View document:

Uphold the 4th Amendment. Only examine records of people when you have CAUSE to look closer. Do NOT look at everyone as if we are all guilty!

---

Comment Submitted by Zackery Conelley

Comment

View document:

Anyone who thinks this initiative will have any positive effect simply is an idiot. We have a record, currently of \*zero\* provable successful prevention of any terrorist incident(s) via information gleaned in any of the incredibly intrusive and unconstitutional methods already employed.

---

Comment Submitted by J. Michael 'Mike' Henderson

Comment

View document:

This searching of our online presence violates our right to privacy, and is a violation of the 4th Amendment prohibition of unreasonable searches and seizures. It is wrong.

---

Comment Submitted by Anonymous

Comment

View document:

I think that sounds completely Orwellian and I fervently hope you abandon this plan, in the name of democracy and freedom of speech. Not to mention freedom of association.

---

Comment Submitted by Wendy Crawford

Comment

View document:

The internet should not be used against us. Things can be misconstrued, taken out of context, if you've had a bad day, etc. This is Orwellian.

---

Comment Submitted by Pamela Gude

Comment

View document:

the only reason i checked no on a lot of these is because WHAT?!? hell no! was not an option.

---

Comment Submitted by Kevin Conway

Comment

View document:

I come from a country with a different political system where we have more freedom to speak.

---

Comment Submitted by R Gorman

Comment

View document:

The department of homeland security and the TSA should both be shuttered with a return to a realistic and practical approach to security. Crime is down in this country- stop the cowardice, fear, paranoia and and hate being spread by the politicians and the press.

---

Comment Submitted by Matthew Glover

Comment

View document:

My own online presence is immaterial, but many people hide their online presence for good reasons, whether it's their own safety, or the safety of those around them, demanding that information puts a cooling effect on travel, which will only increase the tribalism and issues that is causing around the world

---

Comment Submitted by Alice Beauchamp

Comment

View document:

Even George Orwell would be astonished if that came about.  
Out of question if supposed to be a Democracy!

---

Comment Submitted by Henry Dale

Comment

View document:

My online presence is private information, protected by the constitution of the U.S.A.

---

Comment Submitted by James Horton

Comment

View document:

My right to privacy includes to my digital life.

---

Comment Submitted by Vicki Fletcher

Comment

View document:

no security at the expense of freedom

---

Comment Submitted by Mark Arntson

Comment

View document:

No entity or organization has any right to see my online presence without my permission. While I can understand why the US Dept of Homeland Security may want access to every avenue, this information is personal and private and not available those who have no permission to it. Access

to or lack of access to this information should have no bearing on my ability to enter or re-enter the United States or any country.

---

Comment Submitted by Jacob K. Doe

Comment

View document:

I think its fair enough for security reasons.

---

Comment Submitted by David Friedman

Comment

View document:

As a United States citizen I have the right to privacy and free speech without government interference.

---

Comment Submitted by John Bethencourt

Comment

View document:

This proposal is an appalling, life-changing invasion of privacy that is in no way necessary or justifiable on the basis of the threat of terrorism.

---

Comment Submitted by R. HD

Comment

View document:

This is a clear violation of free speech and should never have gotten past the brainstorming stage. Shame, shame for selling our freedoms so cheaply.

---

Comment Submitted by Christina DeVries

Comment

View document:

Governments should not have access to our private conversations, absent legitimate probable cause for such investigation.

---

Comment Submitted by Bob Fawcett

Comment

View document:

Is this a Donald Trump proposal? If the US was like this I would never want to visit again. I'd spend my money travelling elsewhere.

---

Comment Submitted by William Boardman

Comment

View document:

Police state methods are anathema to a free society.  
Got a problem? Get a warrant.

---

Comment Submitted by Sylvia Barnard

Comment

View document:

This is a big infringement of rights to privacy and a real terrorist wd not exactly post their plans on Facebook.

---

Comment Submitted by Peter Childs

Comment

[View document:](#)

I think we've gone much too far already in prioritizing security over privacy.

---

Comment Submitted by Frank Evelhoch, II

[Comment](#)

[View document:](#)

I think this idea stinks.

---

Comment Submitted by Jennifer Foster

[Comment](#)

[View document:](#)

This seems to be a thinly veiled attempt to target at Muslims. Furthermore, who would be vetting information found, and what threshold would be used to deny entry of an individual in the country? There are plenty of individuals in the US who post violent rhetoric directed at women, people of color, and religious groups. The threat of violence is primarily coming from within the borders of the US--the DHS would be better served to pay more attention to gun advocates and prevent individuals from accessing deadly weapons within the borders.

This proposal also invites way too much subjectivity into the process of obtaining a visa. How would officers be trained? Would one flippant comment be enough to prevent someone from entering the country? How and when would people be notified of a denial of entry and how long would an appeal take?

---

Comment Submitted by Johan Greefkes

[Comment](#)

[View document:](#)

Even with the field marked optional, entering the country is already a very hostile and intimidating experience, visitors will not understand and feel obligated to complete. Bad guys will know or provide false or 'safe' information. The end result is that the haystack becomes bigger without adding needless to find. A lose lose scenario.

---

Comment Submitted by David Guy

Comment

View document:

it sucks

---

Comment Submitted by Leah Catania

Comment

View document:

This preposterous. The government should not have any more access to social media accounts than they would get if they Google your name. If people choose to set their information to public, and it is visible through a general search, then it's free to access by whoever, the government or anyone else. But anything that you have set to private or friends only should absolutely not be accessed by the government and should not be a deciding factor in whether or not someone gets to come into the US. And the government should not voluntarily ask for it, because most people will feel several pressured to give that information when it is a violation of their privacy rights.

---

Comment Submitted by Michael Arentoft

Comment

View document:

Invasion of privacy to make a government employees job 'easier' is wrong and should never be allowed. It seems to be an outright violation of a persons right to privacy.

---

Comment Submitted by Martha Dingilian

Comment



View document:

I don't think it is right to search anyone's online presence without a reason or warning.

---

Comment Submitted by Henrik Huhtinen

Comment

View document:

The program does not prevent any threat. What prevents anyone unwanted from creating fake profiles that they would provide if this program was in place?

---

Comment Submitted by Dave Harris

Comment

View document:

if they start doing this, I will regard the USA as totalitarian and will not visit there. At the moment, I have planned an 8,300 mile, 3 month trip to visit all of my friends in the continental US and Canada. if this nonsense is put in place, I won't make it. I might go just to Canada & see my friends there. Having said that, if it's restricted to only what I post publicly, I don't see a problem with that. In any case, it's a daft idea - too easy to game. It's trivial to create fake accounts & populate them with a few harmless people & posts, then have just those on your phone when you arrive in the USA. So, a serious waste of money unless the \*real\* idea is to gather a load of information for some other than the declared purpose :/

---

Comment Submitted by Kenneth Hetland

Comment

View document:

To check everyone just to find 1 or 2 that aren't techsawy is not ok. It will only educate the ones that have something to hide to conceal their information on the web.

---

Comment Submitted by Katrina Buskirk

Comment

View document:

This is getting way out of hand. The majority of Americans, and people in general, do NOT spend their day plotting acts of violence against others. TSA and ICE have prevented ZERO terrorist attacks. This is just another unnecessary invasion of privacy against the individual.

So much for free speech and the right to privacy in ones items and papers.

---

Comment Submitted by J Crim

Comment

View document:

I think it is fair to say if you post on social media it can be searched and indexed. If they wanted a username, perhaps however, I do not believe any agent should be given account access. No passwords or means of access should be given. Yes there could be value in searching that information, but we don't need account information ( email, password, authentication methods etc ) available in more locations which could be compromised, let alone agents themselves who can become compromised and share that information nefariously. That is not a slight against custom agents, but humans are humans, sometimes under paid and over stressed and things happen.

---

Comment Submitted by Elke Hoppenbrouwers

Comment

View document:

I don't think the government should have the right to inspect by 'online presence' on the other hand I am not sure that they don't do it already.

---

Comment Submitted by Catherine Fitzpatrick

Comment

View document:

I am happy to have you collect any and all data from social media in order to filter it for connections with terrorists and criminal suspects. Since none of the NSA surveillance to date exposed by Snowden and others has been proven to actually expose the privacy of any US citizen or cause any harm to innocent US citizens, I don't see what on earth is wrong with scraping open data.

---

Comment Submitted by Bonnie Faith

Comment

View document:

it's unconstitutional

---

Comment Submitted by RJ Godin

Comment

View document:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

---

Comment Submitted by Robert Cassinelli

Comment

View document:

The US DHS should heed the words of the Constitution regarding due process. Show me probable cause for the need to scan my social media and/or networks, and they and my attorney can discuss this. After said discussion, my decision should be considered final and irrevocable until/unless new information, verified and vetted as to likelihood of being true and the trustworthiness of the source(s). Otherwise, my choice, my decision, end of subject.

---

Comment Submitted by Donald Di Russo

Comment

View document:

I have no online presence; I think that is all **RIDICULOUS**. It seems there is no such thing as privacy anymore & we do have to keep ourselves safe some damn how. However, I'm not sure you'd be able to search my pockets & wallet without due cause. Oy, I obviously don't know the answer to this one. What do the Israelis do?

---

Comment Submitted by Anita Hernandez

Comment

View document:

This is ridiculous...Everything about the constitution and human rights is being violated. This must not be allowed to happen. It is an obscene violation of privacy..

---

Comment Submitted by David Cramer

Comment

View document:

I'm not interested in keeping track of social media accounts for the sake of an intrusive, paranoid intelligence authority who are searching for needles in a haystack by a hostile takeover of all haystacks. The DHS is infamous for brutal incompetence. Besides that, my only social media participation is based on my need to keep track of other musicians' schedules, enjoy archival videos of other songwriters and performers, and see what friends and acquaintances in my family and in the arts and music world are up to. I don't usually post or participate in any other way. Besides that, if asked what my social media subscriptions are, I wouldn't even know what to include. I don't keep track. So I'm sure I would be regarded with suspicion for leaving some of them out. I assume this would be a problem for most people. We just don't keep track. So a government assumption that we'll all have a handy list ready to turn over to a gestapo (Where are your papers?) will fail embarrassingly. Good luck with that. An even bigger problem is that people are curious about practically everything. Mental health and security conscious people all over the world are trying to make sense of the crazy stuff going on in the world by following links and signing up for information. The DHS has no concept of the randomness of human curiosity; but will be tempted to follow up every single link from every human being on the planet, instead of doing actual police work. More community police work everywhere would be

a lot more valuable than secret, extra-legal, unaccountable, military intelligence styled invasions of privacy.

---

Comment Submitted by John Holt- Carden

Comment

View document:

Just make sure no one enters the country with a bomb. You have enough problems doing that. Leave the rest alone.

---

Comment Submitted by Rebecca Egipto

Comment

View document:

Please read the 4th Amendment

---

Comment Submitted by Lori Carlson

Comment

View document:

I am not willing to sacrifice my right to privacy nor this ridiculous amount of tax dollars just so some border guard can use my social media posts to make a bad decision about me.

---

Comment Submitted by Gordon Brown

Comment

View document:

I think that such measures remind me a lot of my childhood, growing up in the authoritarian Assad regime in Syria.

---

Comment Submitted by Cathy Brownlee

Comment

View document:

Not without a warrant

---

Comment Submitted by Leen Bekink

Comment

View document:

Bad plan

---

Comment Submitted by Robert Costa

Comment

View document:

It reminds me much of the Robert Oppenheimer case in the 1950s when despite all that he did for the U.S. he suffered from major oppression by the government just because some of his friends had connections to communists. Similar things are bound to happen here :(

---

Comment Submitted by Dr. Alexander Henrich

Comment

View document:

Leave us be, your job is not harassing blameless people just for wanting to visit your country!

---

Comment Submitted by John Byrnes

Comment

View document:

This plan is a violation of privacy and in no way makes the US Border any safer, it creates a government controlled program that can compromise individual digital resources. Given the

failure of usajobs.gov to protect federal employees private data, I would I n no wau trust a more comprehensive database with no clear puroose other than surveillance.

---

Comment Submitted by Andrea Cain

Comment

View document:

I don't participate on any social media. I feel as though the technology is not secure and never will be.

---

Comment Submitted by Joyce Hansen

Comment

View document:

These types of intrusions invade our privacy. They take away our freedom of speech and assembly rights without due process. No one should be spied upon without a warrant issued by a judge for cause. These programs do nothing but instill fear, and stifle free thinking, actions and innovation. It is unconstitutional regardless of what laws or regulations our government and its representatives pass. Everyone on social media exaggerates, lies, gets angry and expresses themselves, just to get noticed. Social Media is not an accurate representation of the person, it's more like being whomever you want, a big game and does not reflect the actual person. Most of social media reflects fantasy and people would never do or say the things they do on social media in person or face to face. That's why people use social media, because it's anonymous. Surveillance needs to be done the old fashioned way and social media will give you nothing, most of the time. Good surveillance takes informants, money, intelligence, patience and a warrant. Do your homework.

---

Comment Submitted by Joe Croft

Comment

View document:

I have little 'presence' online as it is. If this goes through I will remove those few things that I do have.

---

Comment Submitted by G Gurka

Comment

[View document:](#)

It is an invasion of a U.S. citizen's right to privacy.

---

Comment Submitted by Brooke Biggs

Comment

[View document:](#)

This is unAmerican.

---

Comment Submitted by Edward Costello

Comment

[View document:](#)

I am a US Citizen who travels routinely outside the US for business and leisure. Any plan by the US to request or require such information would be immediately turned upon American Citizens traveling abroad. A serious concern would be that information which is legal and Constitutionally protected speech in the US would be used against US Citizens traveling abroad, not only to reject entry in a foreign country, but potentially to impeach or indict Americans abroad for Constitutionally protected speech written at home on social media.

---

Comment Submitted by Ethan Grabowski

Comment

[View document:](#)

I understand that the right to free speech is not the right to free speech without consequence. However, this seems like several steps too far concerning government over watch. The NSA probably already has this information, but requiring a check of social media just to get into a country is too far. I'd prefer not to live in the world of 1984.

---

Comment Submitted by Michael Gnat

Comment



View document:

Unless you have good cause to believe a particular individual is engaged in anti-US terrorist activities -- in which case a warrant should definitely be obtainable & obtained -- one's online presence should be left alone.

---

Comment Submitted by Stuart Dean

Comment

View document:

An absolute disgrace and an affront to democracy! The right to anonymity is an essential part of democracy! Even the US Foundling Fathers were in full agreement with that.

---

Comment Submitted by Catherine Bantigue

Comment

View document:

It's a waste of time and resources that can be put to better use. The vast majority of people use their social media accounts to share either mundane or amusing things. So that's a lot of time and money spent pulling people aside to clarify information taken out of context since neither the public nor the government are the intended audience. And while people are busy clearing their names, actual criminals and terrorists can better fine-tune their methods to work around these procedures yet again.

---

Comment Submitted by Catherine Bell

Comment

View document:

As a natural-born American (U.S.) citizen, I am opposed to using social media as a tool to keep people out of the country, especially as such action will likely be turned against U.S. citizens. We have a Constitutionally guaranteed right to freedom of speech, which includes prohibitions decided by court cases against the chilling of it. Given how very poorly people understand each other in general, the idea of using social media as a gauge of who is and is not a threat is both

terrifying and ineffective. If the government wants to check social media activity, there are other ways to do so (and that are already being done) that are more targeted, more accurate and less disruptive to travel than searching people's brain-spaces at the border.

---

Comment Submitted by Michael Cote

Comment

View document:

I want the social media information of every government employee, not the other way around.

---

Comment Submitted by Erik Hermansson

Comment

View document:

Bad idea.

---

Comment Submitted by Nikolay Dyulgerov

Comment

View document:

This is seriously endangering free speech and online freedoms. Not to mention that even if a person is completely safe and sure about his accounts, and gives them to the Homeland Security, he will probably still feel humiliated, as he would not know what might happen to him and his accounts.

---

Comment Submitted by Kenneth Campbell

Comment

View document:

Absurd.

---

Comment Submitted by Mark Dalton

Comment

View document:

I choose who sees what I put on Facebook. If I want you to see it, I'll post it as 'Public'. Otherwise, do not invade my privacy.

---

Comment Submitted by Alberto Arnoldi

Comment

View document:

There's no need for Intelligence agencies to scan social media to determine if a person is suspicious or not.

---

Comment Submitted by Tim Howard

Comment

View document:

I support privacy rights. leave my social media alone unless you have a warrant!

---

Comment Submitted by Herr Flupke

Comment

View document:

What people post online is only a very limited representation of who they are (and thus whether they are a threat to the US). People post online to project a certain image to their immediate peers. This image depends on the context. Think an online learning platform vs. a social space to hang out online vs. a site dedicated to recovery from illnesses etc. This image also depends on the perceived peers/audience. Most people talk differently (in choice of topics and words) when

communicating with their close friends vs. being in public. It is accepted to go on exaggerating and polemic rants in private (e.g. over a drink at a friends house) vs. laying out a nuanced argument against a certain subject.

If the U.S. Department of Homeland Security is going to use the online presence of a person to judge them (which is the end result of searching the online presence) it is going to eat fruits of a poisonous tree.

First: guilt (purely) by association. What if a number of my peers (of my online presence) are not welcome to the US. Am I also not welcome? What is a reasonable threshold? (see also small-world experiment) The hidden assumption is that I am like my peers. But there are very good reasons to communicate with others having wildly divergent world-views, if only to learn about them.

Second: people change. How will the DHS (or anyone else) determine that something posted in the past is still an accurate reflection of the current intentions of a particular individual? Two (simplified) examples: Should an America-hating individual be allowed to enter, just because they liked Coco Cola in the past? Should a (past) critic of US policy be denied entering the country just because their views are not in line with the US government? How much deviation would be acceptable?

Third: the DHS will be tricked. A terrorist could create a US-friendly online presence to increase the chance of being admitted into the US. Someone could create fake profiles just to (indirectly...

---

Comment Submitted by Thomas Askjellerud

Comment

View document:

No way!

---

Comment Submitted by Sharon Hilchie

Comment

View document:

It's an encroachment on our freedom of speech. It would hopefully be overturned in the supreme court. There are much better things to spend this money on.

---

Comment Submitted by Colin Doran

Comment

View document:

Not a lot. I will never, touch wood, be visiting the country.

---

Comment Submitted by Melinda Fries

Comment

View document:

I think this would be a complete invasion of my privacy.

---

Comment Submitted by John Carter

Comment

View document:

The government is welcome to conduct searches of people's social media accounts in any way they are able to without the public giving them any information on those accounts. Yes, the government should absolutely investigate, and it should also never ask the public for their account information.

---

Comment Submitted by Douglas Henderson

Comment

View document:

Bad idea. Focus on our government corruption like the sleazy Clinton Foundation.

---

Comment Submitted by James Bengel

Comment

View document:

First, and probably foremost, only an idiot would post intent to engage in terrorist activity on social media, and odds are the US Government already knows about the dumb ones anyway. Second, there is no vetting by social media platforms to ensure that the account actually belongs

to the person it appears to represent. ANYONE can set up a Facebook account, under an assumed name so any intelligence value gained from it is at best suspect. Third, the browsing habits and history of anyone accessing the internet anywhere are already catalogued so that Google and others can make money. At best, you gain questionable information and at worst the sheer volume of data makes a haystack so vast that the needle is lost forever. Finally, freedom of expression is (for now anyway) a cornerstone of the American system of government. It is enshrined in our Constitution as the first line item of the Bill of Rights, so the framers must have thought that it was pretty important. Arguably the Constitution applies to US citizens alone in a legal sense, but principle is not limited by geography. A thing is either right or it is not. And if recent history has taught us nothing else through the candidacy of Donald Trump, it is that as a nation we believe that even the vilest insult has a right to be heard.

---

Comment Submitted by Frank Ackerman

Comment

[View document:](#)

This is the height of government interference of our rights as a free people. Only a court should decide if there is just cause for our rights to be violated. Not a government flunky.

---

Comment Submitted by David Hare

Comment

[View document:](#)

This is a horrible idea - a sure way to perpetuate a culture of fear and suspicion, without actually making anyone safer.

---

Comment Submitted by Larry Daniell

Comment

[View document:](#)

No, don't search my on-line presence. American is about freedom. That's it. You spy, American citizens lose freedom!

---

Comment Submitted by David Gustafson

Comment

View document:

The Department of Homeland Security should not be able to access a person's online presence every time you enter the United States.

---

Comment Submitted by Stephen Dickinson

Comment

View document:

Big Brother is watching you.

---

Comment Submitted by Andrea Frankel

Comment

View document:

I shudder when thinking of the prior restraint on free speech that your new policies would create. I do not trust DHS to make wise choices about granting entry to the US based on what is posted on social media accounts.

---

Comment Submitted by Anton Feenstra

Comment

View document:

It is downright horrifying. It's reversed evidence: guilty until proven innocent - or maybe rather guilty until assumed suspect.

---

Comment Submitted by Blanu Bisli

Comment

View document:

It's an abomination, I'd rather stay away from the US.

---

Comment Submitted by May AbdelRazik

Comment

View document:

I don't know which part of 'personal' doesn't the U.S. Department of Homeland Security understand. This is obviously a violation of my Human Rights, my right to a private life. What I say on my social media account among my friends, should NEVER be read by anyone other than my friends, how is this any different to tapping on my phone conversations without a judge's order

This is absolute madness and if the world turns into this then we need to stop using social media all together.

---

Comment Submitted by Norbert Bollow

Comment

View document:

It would be a strong reason for responsible, privacy-conscious people to avoid visiting the US.

---

Comment Submitted by Kyle Bates

Comment

View document:

Social media posts are far too easy to be taken out of context and misunderstood. This alone makes it unsuitable for determining security risks. Reject this plan immediately.

---

Comment Submitted by Kathleen Childs

Comment



View document:

This is yet another form of useless security theatre that will be expensive, unnecessarily invasive, and would provide no useful information from a policing perspective.

---

Comment Submitted by Carmen Christgau

Comment

View document:

I will delete all my accounts before I let this happen. That's the most polite answer I have. This is infuriating and unconstitutional.

---

Comment Submitted by Anonymous

Comment

View document:

I believe that this plan is going to backfire because people who are already in our country, who were born here, are going to find this a huge violation of privacy, kinda like we did with the whole NSA thing.

---

Comment Submitted by Terry Gruzebeck

Comment

View document:

I'm a U. S. citizen. I was born in the U.S., and I've lived in the U.S. all of my life.

As an individual member of America's collective popular sovereign, the federal (U.S.) government owes We, the People, who duly ordained the very existence of the federal government, together with an absolute duty of obedience and allegiance, and its absolute good faith and true fidelity in securing and promoting the rights and prerogatives of all U.S. citizens (whether constitutional in nature, or derived from federal statutes) as against those internationally-recognized rights and interests of all other governments and peoples of the world, a pledge to never legislate public policy in its own hegemonic interests, insofar as there must never be even so much as an appearance of either a conflict of interest, or any other improper relationship between the federal government and its collective popular sovereign, so help you, God.

And if any government agents, federal or otherwise, want to know something either about me, or about any other U.S. citizen, get a proper search warrant, the particulars of the probable cause upon which it is predicated thus being founded on reasonable grounds and fundamental fairness, and also being fully transparent and knowable, and also being independently and objectively verifiable, and also being subject to the rigorous scrutiny of both procedural and substantive due process under both the 5th and the 14th Amendments, and hence, being fully challengeable in open court.

Government secrecy is the breeding ground of corruption and defalcation, the harbinger of intrusion, and the handmaiden of unresponsive entrenchment and tyranny.

---

Comment Submitted by Jeff Holquist

Comment

View document:

If you suspect that someone is potentially a threat, go tell a judge and get a warrant. It's really that simple.

---

Comment Submitted by Christian Hyer

Comment

View document:

Extremely bad. Reminds me of Soviet Union methods, the Stasi way of spying via friends and family.

---

Comment Submitted by Michael Garber

Comment

View document:

The chilling effect that such a requirement would have on free speech, both for American citizens inside the country who will cross the border and for non citizens entering the country, would negate whatever supposed intelligence gains such a policy would bring.

---

Comment Submitted by Cristi Craciun

Comment

View document:

I don't want U.S. Department of Homeland Security to search my "online present".  
Thanks.

---

Comment Submitted by Patricia Greenough

Comment

View document:

Talk about Big Brother. It's insane, all this documentation frenzy. US government resources already monitor radicals websites & shut them down, & other questionable sites. Adding to more wait time in screening & customs just increases the discomfort of travelers. If the US government is already monitoring radicals what makes them think they'll get any more information from social media? Who of radicals would be so foolish to post radical posts or comments on social media where they're already being monitored? Due to some terrorists the rest of humanity gets to be suspected of being radical & gets treated badly by poorly trained, officious airport security people. I won't fly anymore due to an experience of being frightened by airport security as the rings on my fingers alerted them for a body search. They told me afterward if I'd put my rings in my purse where x-rays would show the rings, that I wouldn't have been pulled out of line & taken to a room for a body search.

---

Comment Submitted by Chris Goldberg

Comment

View document:

I have no social media presence. I cancelled a Facebook account because of Facebook's overreach. I decided that the only way to have privacy in this society is to stay analog in my communication with others. Will saying I have no social media accounts at the border brand me as a freak and send me to the little room with the man in the rubber gloves?

---

Comment Submitted by Alan Arnold

Comment

View document:

Customs is not the CIA, NSA, etc. Law enforcement agencies can properly perform these activities with a legally obtained warrant.

---

Comment Submitted by Lucas Dixon

Comment

[View document:](#)

I think this is a violation of the right to free expression and the right to free association; I think the US should not jeopardize social freedom by asking people to identify their statements and associations before entry.

---

Comment Submitted by Rick Hart

Comment

[View document:](#)

Only if you get a warrant. You're sworn to defend the Constitution. Do your job and leave people alone.

---

Comment Submitted by Matja Demar

Comment

[View document:](#)

Social media accounts are often an expression of personal interests, hobbies and activities, which during an analysis would raise false flags. It should be an optional step, if someone is investigated. But we must not forget, that online accounts can be made up and tailored to use. So, while innocent travelers could be false flagged and marked, attackers would most likely use false accounts, if needed. Overall, this approach would just burn money and create probably just a false sense of security.

---

Comment Submitted by Aaron Eiche

Comment

[View document:](#)

Online Presence is a mixed space. It represents only a facet of an individual, the portion they choose to represent as themselves online. That representation may change depending on the audience. Without that relevant context (which is impossible for the Dept of Homeland Security

to determine, because it's based on an individual's experience), analysis of online presence will inevitably yield inappropriate information, or malformed interpretation of information. It will lead to misinformed and inappropriate actions at our borders.

---

Comment Submitted by Diana E Forrest

Comment

View document:

This will deter me and many others from entering the USA. Such information can be used in many ways other than preventing terrorism and could be used to limit lawful political activity in the USA and elsewhere.

---

Comment Submitted by Dave Bush

Comment

View document:

Stupid

---

Comment Submitted by Erin DeSpain

Comment

View document:

Freedom to move and choose ones residence is a basic human right. Freedom of privacy is a basic human right. Freedoms of thought and communication are basic human rights.

This provision, whether voluntary or not, subjects individuals at borders (potential refugees) to scrutiny where their basic human rights may be abused directly, if they comply, or indirectly, if they do not acquiesce to requests for their social media information.

People entering the US have basic human rights to not be subjected to this kind of scrutiny.

We are either a nation who supports basic human rights or we are not. This proposal by the DHS implies that we are willing to violate the basic human rights of migrants, businesspeople, and refugees. While the intention of this proposal may be good (to prevent potentially dangerous individuals from entering the US) the method of requesting this kind of information sets a precedent even more dangerous to the freedoms of US citizens, and would-be citizens and residents, that their information and affiliations can be scrutinized by individual officials, or computer systems, who can determine whether or not these individuals will be granted basic

human rights that the US is already obliged (or should be obliged) to honor and respect.

In short, this proposal represents the potential elimination of basic human rights people in general already enjoy. It's advancement as a proposal is deeply disturbing and clearly represents a willingness to sacrifice the American ideals that have made our nation great for the momentary bureaucratic convenience of DHS personnel at our borders. Sadly, this proposed program also sounds like another in a long line of boondoggle spending programs that increase in taxpayer costs without a sufficient evidence of commensurate increase in taxpayer benefits.

We should be spending this money on education, welfare, or the real tangible benefits of ordinary citizens (or by lowering their tax burden) than by...

---

Comment Submitted by Kevin Hickman

Comment

View document:

It is too easy for individuals and agencies to move from useful analysis to abusive use of such information. The Soviet Union tried to gain all information possible on its citizens and we viewed it as evil then. The act is no less evil, just because the US is trying to implement it now.

---

Comment Submitted by Shahid Buttar

Comment

View document:

As Americans, we are entitled to the right to speak freely, both for the sake of our individual freedom and to safeguard democracy from the chilling effects of government scrutiny. Government monitoring of social media undermines both free speech and democratic norms, and even more so if acquiescing to monitoring is presented as a requirement of re-entry to one's own country. Our Founders would roll in their graves were they still alive.

---

Comment Submitted by Dennis Giesbrecht

Comment

View document:

equal rites for all us & them . free thought do no harm must be the goal for all . not infiltrate, concur, under-mind peaceful societies solely for the purpose of slavery is not any mans right to

impose on another. ones life is not free for the taking by another . snooping in ones views by force or demand is a terrorist act perpetrated by anyone no matter what the goal might be by those who chose to venture down that path . we should be able to know what there are doing if they must know what our thoughts are . equal rights for all ,or is it clear we now have no rights left as it is in the now ?

---

Comment Submitted by Jane H Beattie

Comment

View document:

surveillance does not make anyone safer; it just allows removal of rights

---

Comment Submitted by Anonymous

Comment

View document:

If your goal is to demonstrate that the United States is the most fearful country in the world, afraid of shadows and bogeymen, this plan will help. Otherwise, you should try doing something that will actually help without appearing straight out of a George Orwell dystopia.

---

Comment Submitted by Milton Horst

Comment

View document:

This would be a serious invasion of privacy and should not be allowed.

---

Comment Submitted by Tom Flemming

Comment

View document:

The U.S. Department of Homeland Security is casting its net too broadly in seeking to examine the online presence of every foreign visitor.

---

Comment Submitted by Peter Berry

Comment

View document:

Several of the answers I gave to this survey are no because of the possibility for abuse and mistaken identity. I see no issue with checking recent posts and contacts provided those posts and connections are public, it can be shown that the account is definitely the person in question, and any records are destroyed once they are no longer needed (in accordance with widely accepted data protection principles). Denying entry on the basis of refusal to provide accounts is unacceptable because billions of people, including in developed countries, don't have them - it would discriminate against them. I am also fundamentally opposed to infringement of third party privacy as would happen if second degree connections were analyzed.

---

Comment Submitted by Max Farrell

Comment

View document:

The invasion of our privacy only endangers our citizens and partners, it does not protect, I do not feel with the current state of things that the government can or should be trusted with social media account access

---

Comment Submitted by Petter Blomberg

Comment

View document:

Will I be denied entry to the US for sharing opinions with the wrong presidential candidate? No? How can you be sure that will not be considered dangerous in the future?

---

Comment Submitted by Mikki Chalker

Comment

View document:

This is ludicrous



---

Comment Submitted by Ellen Graubart

Comment

View document:

Governments should not interfere in citizens' rights to privacy.

---

Comment Submitted by Andrew Castillo

Comment

View document:

Subjecting one's online presence to arbitrary searching by government agencies sets a dangerous precedent in any free democracy. With such a potentially large database, the danger of false positives is simply too great. We've seen time and again that the issue in preventing terrorist attacks is not a lack of quality intelligence, but an overwhelming abundance of meaningless info. Creating more dots will not make connecting them easier. You don't find the needle by adding more hay to the pile.

---

Comment Submitted by Robert Anzaldua

Comment

View document:

I feel that such a search, particularly when not subject to public oversight, is a violation of the spirit of our First Amendment Rights as U. S. citizens. I don't care that they are not banning certain sentiments; I care that they would make us censor our own thoughts on our own blogs. If I say eff this country out of rage or frustration at current events, I do not wish that statement to be taken as an anti-American sentiment, rather than conscious social commentary.

---

Comment Submitted by Francesca Dickinson

Comment

View document:

It's an invasion of privacy.

---

Comment Submitted by Peter Hessler

Comment

View document:

This is throwback to McCarthy-ism and to the scare tactics of the KGB and Stasi from the Cold War years.

---

Comment Submitted by Chris Crane

Comment

View document:

That's insane!

---

Comment Submitted by Will Hopkins

Comment

View document:

I think it's a terrible idea. It will have a chilling effect on normal, everyday speech, as well as politically sensitive speech. The idea of such a process in the hands of the next administration...I shudder to think.

---

Comment Submitted by Diana Elle

Comment

View document:

A shocking invasion of privacy. I would not give them this information, even if it means that I would be forced to cancel a planned trip. And no, I don't have 'something to hide', I just value my privacy

---

Comment Submitted by Jerry Cassels

Comment

[View document:](#)

I would be perfectly comfortable with this as I have nothing to hide.

---

Comment Submitted by Alexandra Henshel

[Comment](#)

[View document:](#)

No- entirely unacceptable and inappropriate.

---

Comment Submitted by Charles Cox

[Comment](#)

[View document:](#)

I think that it's a ridiculous waste of time to use social media. I don't use them (either sending or receiving). The rest of the world doesn't need to know that level of detail about what I had for dinner or who or what I'm visiting. If the CIA has found it useful to search social media to find people who want to harm US or its citizens, let it do so in secret for as long as it can (until another Snowden comes along) and then it can explain its activities in a secret court and get approval or not to continue. Since we don't know how effective searching social media would be, let's get some data (without telling the public) and then make the decision. But, let's not fool ourselves into thinking that govt. legislation is going to solve this problem. From a time parameter, we're a little late for what's described in the book 1984, but make no mistake we're going to be there by 2024 (40 yrs late!). And, note, that once the terrorists know that these social media accounts are monitored, they will use newer technology to circumvent the legislation...and the cat and mouse game will continue. What we (the govt. and the scientific community) ought to concentrate on is studying why people become terrorists. Study Eric Hoffer's book, The True Believer, and spend whatever it takes to understand why a person goes off the rails.

---

Comment Submitted by Diana Holmes

[Comment](#)

[View document:](#)

If you are not a US citizens you do not have the same rights.. I'm on the fence about a lot of this I also believe we have the right to protect ourselves., please keep me updated. I may change my thinking along the way...

---

Comment Submitted by Matthew Eargle

Comment

View document:

First, as a taxpayer, I feel that it is an unnecessary waste of federal money that could be going to critical infrastructure investments or other, more appropriate spending avenues. Secondly, I feel that it is a grievous injustice to demand unfettered access to private information for the sake of a surveillance dragnet that has proven itself ineffective at protecting the people of the USA. As a philosophical matter, the USA is--historically--the bastion of freedom and the antithesis of police states such as East Germany or the USSR; to enforce new social vector analysis on visitors (or, worse, returning citizens) would make us no better than the oppressive regimes that we purport to oppose. As a practical matter, this would cause Customs inspection lines to increase geometrically and lead to decreased economic activity in the tourism and hospitality sectors among others.

---

Comment Submitted by Richard Cardona

Comment

View document:

Monitoring online social media presence will force the creation of more anonymized social media action like a Tor for social media.

---

Comment Submitted by Kevin Brown

Comment

View document:

I frankly find it a detestable invasion of privacy, and almost comically tone deaf in an age where online privacy concerns are an issue. I additionally have absolutely zero faith in the ability of any and all federal government agencies to actually detect potential threats entering the US, and given the quality of ethics and morality displayed by many government officials in recent years I do not trust them to use any information gathered for good.

---

Comment Submitted by Jani Burgess

Comment

View document:

It's ridiculous and an atrocious waste of time and resources. Have you seen the sorts of crap available on social media. I highly doubt this would be more helpful than cumbersome. What nosey busybody came up with this idea?!

---

Comment Submitted by Samuel Handley

Comment

View document:

No government of the United States has or should ever have any authority over any individual except as specified through due process, in a court of law and following conviction by a jury of peers. Entering or leaving any of the United States only involves citizenship status, legal right to travel and existing criminal convictions. It is not an invitation to go fishing for evidence against innocent people simply because they are caught in an artificial, government constructed, bottleneck.

---

Comment Submitted by Olivia Benveniste

Comment

View document:

That's thoroughly ridiculous. By all means, judge me by the facebook account I've hardly touched since high school, or my tumblr full of Steins;Gate fanart; I guarantee none of that information is going to be useful. This is just invasive for the sake of being invasive.

---

Comment Submitted by Jesse Davis

Comment

View document:

Government use of information should be accessible only after being granted a warrant to do so in a public court, or federal court whose records are accessible to the public immediately.

---

Comment Submitted by B. Ross Ashley (2nd Comment)

Comment

View document:

You can sit on it and rotate rapidly. If you subject me to this nonsense to re-enter the land of my birth, I will cease to spend money South of the Lakes, and encourage a travel boycott campaign.

---

Comment Submitted by Peter Costantini

Comment

View document:

Very bad idea. This is another dragnet, catch-all approach to intelligence gathering. It will not catch potential terrorists, but it will chill legitimate debate.

---

Comment Submitted by Horst Herb

Comment

View document:

An unbearable drift into uncontrolled totalitarianism. Unworthy of any democratic country.

---

Comment Submitted by Hugo Durantini

Comment

View document:

If you are following the rules you have nothing to worry about. Of course, that don't means what our information should be open for access or any type of use without our permission first.

---

Comment Submitted by David Campagna

Comment

View document:

it's none of your business

---

Comment Submitted by Stephan Armstrong

Comment

[View document:](#)

DHS is a duplicate agency that was only started because Bush felt the necessity to make himself look like he was doing something important. They should be disbanded.

---

Comment Submitted by Robert Hicks

Comment

[View document:](#)

This sounds like a police-state policy. If adopted, it will severely damage our civil liberty rights.

---

Comment Submitted by Colin Carr

Comment

[View document:](#)

It is a gross intrusion into my private communications.  
If they have reason to believe I have committed a crime, they should apply to the appropriate court for a specific warrant to examine my online presence. Otherwise, they have no right at all to examine it.

---

Comment Submitted by Beverly Heard

Comment

[View document:](#)

Feels a bit reminiscent of behind the iron curtain in the mid 20th century. We frowned on wholesale snooping on the public then. So why should it be okay now?

---

Comment Submitted by Chris Hardwick

Comment

[View document:](#)

The reputation of the U.S. is at an all time low, with plans like this it is hardly surprising that peoples opinion of a once great country continues to decline. It's about time the U.S. realised that

invasions of privacy are not welcome and will do nothing to enhance security or their reputation in the wider world.

---

Comment Submitted by Jessica Crowe

Comment

[View document:](#)

Bad policy. Do not enact it.

---

Comment Submitted by Elene Gusch

Comment

[View document:](#)

This is sickening. I don't know what the best way to keep terrorists away is, but this can't be it. I think if anything it would just breed more resentment.

---

Comment Submitted by Faith Franck

Comment

[View document:](#)

i think it's a terrible Orwellian idea. I don't want to live in such a world.

---

Comment Submitted by Samantha Bird

Comment

[View document:](#)

Nothing to hide, so how can it be a bad thing?

---

Comment Submitted by Michael Chen

Comment

[View document:](#)

Going over the last few weeks of social media activity is reasonable IMO, any more is a little overboard. Virtually everyone goes through phases in life, but that doesn't always define who



they are right now. Also, the current youth generation consider following a person's online activity, medical record, etc a form of stalking, so it's probably not a good idea follow through.

-----

Comment Submitted by Chris Ayres

Comment

View document:

It appears to me as a lawyer that the USA authorities are not cogniscant of UN policies on privacy and mores importantly of the Declaration of Human Rights.

Should such abusive anti-privacy policies be put in place it would be a powerful argument for my avoiding ever visiting the US of A.

I am not afraid to put my name to what I believe , having, as a retired lawyer and senior citizen of the UK and Australia, nothing to hide.

Chris Ayres

-----

Comment Submitted by Bruce Hogben

Comment

View document:

I assume that we are monitored by governments, but I don't approve of it. I believe we all have a right to privacy. Monitor people who are genuine suspects of wrongdoing, but not everyone.

-----

Comment Submitted by John Gale

Comment

View document:

Firstly who want want to enter the corrupt, second rate USA ? You are in the room of mirrors and do not know how to accurately assess any information you have or may get. Giving you more information will not improve that situation!!!!!!

-----

Comment Submitted by Charlie Green

Comment

[View document:](#)

This is unconstitutional and should not be allowed.

---

Comment Submitted by Herman Goering

Comment

[View document:](#)

It's nazi like.

---

Comment Submitted by Maarten De Waal

Comment

[View document:](#)

This goes way too far. It is a degrading and totally unnecessary violation of privacy, that can get people in trouble for no good reason. These kind of measures only lead to an enormous bulk of mostly useless data, that take a big effort (and a lot of money) to collect without making the US any safer. Old-fashioned intelligence work, done by capable and discrete agents, leads to much better results than these kinds of intimidating 'Big Brother'-measures that show a total lack of respect for human dignity.

---

Comment Submitted by Anonymous

Comment

[View document:](#)

It is a waste of taxpayer dollars for DHS to build a program to study the online presence of people crossing our borders. It is not clear how such an expense could be justified.

---

Comment Submitted by Richard Fish

Comment

[View document:](#)

Social media searches should require a search warrant just like any other search.

---

Comment Submitted by Patrick Burroughs

Comment

View document:

The DHS and the rest of the US Government have neither the right nor reason to view, store, analyze, and correlate the social media information of travellers and citizens beyond that which is already publically available, unless they undergo due process and obtain the warrants and writs required by law.

---

Comment Submitted by Marya DeBlasi

Comment

View document:

How dare you.

If this is not the definition of illegal search then the term itself is meaningless.

Stop the creeping fascism that has overtaken the heart of our democracy.

Say NO to the search of social media accounts of people entering the US or any other democracy.

---

Comment Submitted by Casey Gibson

Comment

View document:

If they already have reason to suspect a person, then they should ask for that information in a later private interview. To request that information on a form is overzealous and unnecessary for the whole of people coming in and out of the country. No wonder the program costs so much; it's requesting millions of people's information that would then have to be aggregated and cataloged, not to mention all the new entries each day to each social media account. That's an insane amount of work and manpower for not a whole lot of return.

---

Comment Submitted by A Barber

Comment

View document:

The US should not be searching online presence. If you have no reasonable suspicion based on real evidence from non-social-media sources, there is no reason to dig into this data. That said, I'm sure they are already using social media to track people they have labeled as suspicious, and I already keep all accounts as private as possible. As I'm sure any real criminal would also do!

---

Comment Submitted by Walker Bennett

Comment

View document:

I do not carry any electronics when entering the U.S. (they can be confiscated without cause), I keep a duplicate smartphone in the U.S. and can retrieve my SIMM info from backup on a foreign (non-U.S. server). All of my Internet interaction is conducted using extreme encryption of my own design.

---

Comment Submitted by Bill Blank

Comment

View document:

It is fascist and un-American

---

Comment Submitted by Jeff Caslake

Comment

View document:

This is a severe overreach of government. It is unreasonable to ask for such information for anyone entering the United States.

---

Comment Submitted by William Anderson

Comment

View document:

Searching anyones online presence without cause is an invasion of privacy and is contrary to principles of duee process and innocence until proven guilty of a crime. For a government

agency to assume guilt in the absence of a crime or cause is counter to generally held views of the American Legal system.

---

Comment Submitted by CJ Hendrickson

Comment

View document:

This is a modern day Nazi-esque mentality. It's a lot like East German policy. That really frightens me.

---

Comment Submitted by Ruth Coustick- Deal

Comment

View document:

This plan is a complete invasion of privacy, and a violation of free speech. For a country that claims to uphold these values, denying them the moment people land in their country is ridiculous and hypocritical. People should be able to post their views, and personal lives on social media without the expectation that it will be subject to examination. Furthermore, this is likely to enable further biases against minority groups, using their photos or habits as trumped up reasons to delay or deny them entry.

---

Comment Submitted by Brian Hicks

Comment

View document:

A analyzing each person's online presence would be a massive waste of time, money, energy, and resources. It would cause more delays, and other harmful problems, than good.

---

Comment Submitted by Kristin Dziembowski

Comment

View document:

This is supposed to be a democracy.  
Shame! Shame! Shame!

---

Comment Submitted by Robert Campbell

Comment

View document:

They will find nothing of interest so it will be a waste of time and money.

---

Comment Submitted by Peter Halvarsson

Comment

View document:

If the U.S is interested in having me as a guest in the country, I would strongly advocate to not inform a mapping of the person and his/her online accounts. In doing so, the U.S will disconnected itself form the international community of modern western civilization.

---

Comment Submitted by Howard Davidson

Comment

View document:

This is a total violation of the Fourth Amendment

---

Comment Submitted by B. Ross Ashley

Comment

View document:

Makes it much less likely that I will ever visit the land of my birth. My mother's grave. My son. Screw y'all and the horse you rode in on.

---

Comment Submitted by John Duqesa

Comment

View document:

It's an unacceptable invasion of privacy

---

Comment Submitted by Stephanie Allen

Comment

View document:

Our right to privacy is far, far more important than any potential information that \*might\* lead to something to do with terrorism. Respect your citizens!

---

Comment Submitted by Anna Hoyles

Comment

View document:

I object very strongly to this. It is an invasion of privacy

---

Comment Submitted by Tim Hayes

Comment

View document:

If you suspect someone of illegal intent, then go get a search warrant just like the rest of law enforcement

---

Comment Submitted by Ingmar Forne

Comment

View document:

I have nothing to hide, but I have everything to protect.

---

Comment Submitted by Jeffrey Austin

Comment

View document:

There are other agencies that should be sifting through social media for bad actors 24/7, in general. There's no need for Customs to get involved on a individual level.

---

Comment Submitted by Timothy Hof

Comment

[View document:](#)

Constitutional rights should not end at the border. no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. It sounds like you give up your rights if you enter or leave the country. This treats everyone as criminal suspects without probable cause. This defines the act of entering or leaving the country as probable cause - how is that justified without any actual criminal suspicion?

---

Comment Submitted by Piotr Urek

Comment

[View document:](#)

I think that normal person entering the U.S. should not be treated as a potential threat. There is a reason for privacy settings for social media. What we make public is public and accessible and what is private should stay private unless there really is need to reveal this information. Such a thing should only be decided by a court of law.

---

Comment Submitted by Michael Gagan

Comment

[View document:](#)

Homeland security should not be using someones online presence as a factor in admittance to the US because once they start any bad actors will change their ways or lie on the form and the rest of us will be stuck with an expensive, invasive, non working system.

---

Comment Submitted by Simen de Lange

Comment

[View document:](#)

Only when there is a reason to believe the person is a danger to society, should this be allowed, and then not without a court order. It will be known well in advance who will arrive and at what times, so a court order should not be hard to get on suspicion

---



Comment Submitted by Malcolm Duffield

Comment

[View document:](#)

The 'real' villains likely have multiple accounts - or use other secure methods to access them. What is proposed creates a false sense of security and is thus a waste of money, time and public goodwill.

---

Comment Submitted by Elaine Fischer

Comment

[View document:](#)

Obey the 4th Amendment - only search with REASONABLE cause, not just as a matter of practice.

---

Comment Submitted by Ryan Bruington

Comment

[View document:](#)

Social media needs to be taken in context and can lead to false positives if examined for criminality. Probable cause should be a minimum standard for accessing private social media information.

---

Comment Submitted by Ryan Bruington

Comment

[View document:](#)

Social media needs to be taken in context and can lead to false positives if examined for criminality. Probable cause should be a minimum standard for accessing private social media information.

---

Comment Submitted by Joyce Frohn

Comment

[View document:](#)

This is stupid. You are wasting agents time and proving to people that the US is a free or safe country. It will not stop terrorists but tourists.

---

Comment Submitted by David Blakey

Comment

View document:

Not only is this an idea that is totally impractical but it will provide no useful information concerning the security risk of any particular person. There are more than enough tools in place to assess risk to citizens or infrastructure - someone just needs to employ them properly.

---

Comment Submitted by Shana Carter

Comment

View document:

This sounds like a gargantuan waste of time and money.

---

Comment Submitted by Hakan Anderberg

Comment

View document:

It's not really any problem to me since US is definitely the last country I will travel to on the planet. US are right now, by ordinary people and since several years by well informed people, loosing confidence everywhere. It is in fact a dying political culture - the pity is that it is still too few US citizens that are aware, but they will soon wake up - thanks to the pressure on the control systems that the loosing party puts on ... But what should they do?

---

Comment Submitted by Hans Henderson

Comment

View document:

totally abhorrent idea

---

Comment Submitted by Mike Hall

Comment

View document:

Whilst I have nothing to apologise for, my opinions are personal ones, and opinions, in a democracy which supposedly embraces free speech, are there to be heard. If I was to be interrogated upon entry by someone who doesn't know me, my sense of humour or based their view of me through their own opinions of what is funny, acceptable and so on, I would more than likely simply not visit the US ever again.

-----

Comment Submitted by Joan Dugdale

Comment

View document:

In the German Democratic (communist) Republic, the Stasi routinely opened and read the mail of its citizens. Is this the sort of state anyone wants the USA to become? There is no difference in this regard between e-communications and paper mail: both are personal and should be private. It doesn't affect me because I have no desire whatever to go to their USA, but if this should become a common practice of democratic countries, we will find ourselves living in a totalitarian world. God spare us all!

-----

Comment Submitted by Kevin Adrian

Comment

View document:

I think it is ridiculous that the govt. thinks this is okay. It's intrusive and a violation of US citizens rights

-----

Comment Submitted by Miranda Harper

Comment

View document:

If this became policy, there is no way in hell I would visit your country. This is dystopic, fascist garbage that would have no usable data. You can't even run your 'no fly list' the way it was intended.

-----

Comment Submitted by Robin Cook

Comment

View document:

TOTALLY UNCONSTITUTIONAL.

---

Comment Submitted by Delena Gaffney

Comment

View document:

This is another invasion of privacy in the name of security. It is just a means to keep people in fear, compliant and controlled. Any one who thinks this is about keeping the public safe has fallen for your propaganda. The Orwellian name for your department is enough to alert thinking citizens to your real agenda.

---

Comment Submitted by Randall Daugherty

Comment

View document:

Such protocols do more to stifle freedom of speech and invade an individual's personal privacy than to keep us safe. Engaging in such tactics is a slippery slope which invites inevitable abuse and has no place in a democracy.

---

Comment Submitted by Matthew Ferrara

Comment

View document:

I think that this survey lack the nuance to really articulate how most Americans feel about this issue. Like many other things with judicial oversight I am comfortable with the government engaging in a wide variety of searches, but this survey doesn't include that as an option. Further I want to know that any overview is a transparent process that actually is critical of requests and not just a rubber stamp that someone needs to get in order to invade my life.

---

Comment Submitted by Kevin Brown

Comment

View document:

This is unreasonable search and seizure. This is unconstitutional. This is a witch hunt. This destroys our moral high ground as a democracy.

---

Comment Submitted by Courtney Belyea

Comment

View document:

No, privacy is an important part of security.

---

Comment Submitted by Marcos Alonso

Comment

View document:

Taking social media comments, posts and likes and using them out of context to build a profile on someone is not only a very poor indication of who that person really is it also sets dangerous markets that our online presence is being used against us whether we are aware of it or not. Our private lives whether online or not should be ours to share alone and no government should have the right to demand access to it to they access to it secretly and use that information to potentially limit out movement or access to people or places.

---

Comment Submitted by Sherry Halbrook

Comment

View document:

I think it is overreaching to want to scrutinize the social media behavior of every US citizen who is re-entering the country every time they re-enter. That information should be checked no more than once every two years, unless a court/judge issues a warrant authorizing such scrutiny and that warrant is based on probable cause evidence. Some people, such as airline or cruise personnel, must travel in and out of the country very often and they should not be subjected to constant, repetitious intrusions on their privacy without just cause.

---

Comment Submitted by Michael Draper

Comment

View document:

Wrong.

---

Comment Submitted by Robin Adams

Comment

View document:

I think it's a waste of time and money, but I do not see any privacy concerns. Social media accounts are public. If I post something on facebook, it means I want the whole world to read it, attached to my name.

---

Comment Submitted by Amy Harlib

Comment

View document:

4th AMENDMENT - NONE OF THEIR BUSINESS!

---

Comment Submitted by Anonymous

Comment

View document:

None of theirs business

---

Comment Submitted by Caroline Darst

Comment

View document:

OUTRAGEOUS!

---

Comment Submitted by Andrew Ferguson

Comment

View document:

Freedom of speech means that the government cannot arrest, refuse entry to the country, or introduce any sort of consequence for a person who criticizes the government, makes their political opinions known, says anything that isn't dangerous, harmful, intentionally misleading with intent to cause harm to or exploit others, or engages in consensual communication with another person. Even if someone claims to approve of a terrorist organisation, the US government cannot legally do anything to that person as long as they aren't doing anything to aid that group's activities. In addition, things said can be misinterpreted by anyone extremely easily. It is not a solid basis of judgement for permittance to enter the country to look at one's social media accounts. Even if it's optional. It's a terrible idea, scrap it.

-----

Comment Submitted by Matthew Brooks

Comment

View document:

It's foolish and a waste of time and resources - surveillance on a wide spread and indiscriminate basis has never been found to be successful and, on examination, historically results in mission creep.

If you need to ask a specific person, ask them and if you feel you have enough to start a direct probe, then do so, but do so under the guidelines of the Constitution, not according to some absurd regulatory commission's interpretation.

-----

Comment Submitted by Kris Alman

Comment

View document:

If DHS implemented non-targeted search of online presence every time anyone entered our country, it would be prohibitively costly and time-intensive. It would violate the 4th Amendment of Americans. Actual terrorists would learn to avoid social media platforms or plant misinformation. This is not a policy DHS should adopt.

-----

Comment Submitted by Anonymous

Comment

[View document:](#)

Searching years of messages I've exchanged with friends and family, along with pictures of my children, friends, work acquaintances, etc. is an appalling breach of the last shred of privacy Americans can call their own. It would literally be far less invasive to search my home every time I wanted to travel.

---

Comment Submitted by Cory Doctorow

Comment

[View document:](#)

I think that this is an expensive boondoggle that will alienate legitimate and beneficial visitors to the USA.

---

Comment Submitted by Jim Freeberg

Comment

[View document:](#)

I do not agree with searching my online presence every time I, or anyone, enters the country.

---

Comment Submitted by Charlene Felton

Comment

[View document:](#)

This is not a useful strategy to keep us safe. Citizens and visitors have a right to privacy for their lives. Nothing will be gained from this program other than loss of that privacy. Anyone savvy enough to use the internet to contact terrorist groups won't be doing it from their main account, or they will just claim not to have social media accounts. And the idea of barring people from the country because they do not have a social media account is patently ridiculous.

---

Comment Submitted by Peter Bowers



Comment

View document:

First of all, we are not BORN with social media accounts. We don't all have one. Second, the U.S. Department of Homeland Security has ABSOLUTELY NO RIGHT to access my accounts. These accounts can be considered anything from a platform for musicians, a way for friends and family to connect, to see what's going on in the world, to promote a good cause, and even just as a novelty. None of these things should be monitored. None.

---

Comment Submitted by Alix Albert

Comment

View document:

It's a proposal that, as so often, will only hurt people who have nothing to do with terrorism. Those who have bad intent and purpose already know how to hide their tracks. But we all value our privacy, we all have things to hide (albeit not nefarious ones), and knowing this data will be taken and analyzed (and possibly abused), will stifle people's free expression on social media.

---

Comment Submitted by Becky Bond

Comment

View document:

This is an invasion of privacy.

---

Comment Submitted by Lulzim Ajvazi

Comment

View document:

If the US Homeland Security thinks in such a way to Save US and American People from any threat of that kind, by checking entrant's social media, then please God help USA. Till now no any terr. act was prevented so far by surveying people through Social Media. L.A. Illyrian Peninsula

---

Comment Submitted by Roy Blake

Comment

View document:

I'm a Canadian. I visit the United States from time to time, mainly for vacations. I won't do that anymore if such policies are in place. Of course the US can restrict visitors any way they like, but if they do this I will decide I'd rather visit, and spend my money, elsewhere. None of my online comments are dangerous or illegal, but some are intended only for my friends, and are, in my opinion, as private as any comments made in person to them.

---

Comment Submitted by Spencer Adams

Comment

View document:

This is not going to alleviate the terrorist problem. You need a warrant as far as we're concerned.

---

Comment Submitted by Jordan Head

Comment

View document:

This is a ridiculous proposal

---

Comment Submitted by Laura Bordeaux

Comment

View document:

Absolutely NOT!

---

Comment Submitted by MD Abbas Ali

Comment

View document:

Hi.. dear sir/madam

i am md abbas ali, i want to travel to the Bahamas Nassau, i live in Bangladesh and i am permanent resident of bangladesh, that is not fact, there is seen in the website of bahamas government Bangladehi passport holder can visit bahamas without visa, but problem is that when i go to travel agencies for buying ticket there is multi air fly, & there i see transit fly Dubai to New York transit, then New York to Bahamas Nassau the end of my fly, now a question, if i go to New York without any transit visa there will be any problem? if yes then how i get the U.S Transit visa, please help me,

sincerely

MD ABBAS ALI