ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

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)[1] 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."[2] 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

[1] 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.

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

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.[3] She did not do so in public posts prior to the attack, according to the FBI.[4] The government would not have access to private messages and posts by simply knowing applicants' social media handles.[5]

Additionally, when Ms. Malik publicly declared allegiance to ISIS on Facebook after the attack began, she did so under a pseudonymous profile.[6] 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

---

[3] 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/facebook-exec-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-san-bernardino-shooting-began-suspect-posted-isis-pledge-to-facebook/.

quick gossip/prep before I go and destroy America."[7] 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.[8]

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.[9] 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-tweet-about-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/universal-declaration-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."

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 self-censorship, cutting back on their online activity (or deleting it altogether)[10] 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.[11] 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.[12] 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.

long supported universal human rights.[13] In 2006, former Secretary of State Condoleezza Rice established the Global Internet Freedom Task Force to focus on human rights and the Internet specifically.[14] Secretary of State Hillary Clinton gave a sweeping speech on Internet freedom in 2010.[15] 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."[16] The State Department continues to actively promote Internet freedom today.[17]

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.[18] 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

---

[13] *See, e.g.*, International Covenant on Civil and Political Rights, https://www.congress.gov/treaty-document/95th-congress/20 (signed by the U.S. in 1977 and ratified by the Senate in 1992).
[14] 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.
[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-kerry-delivers-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.

activities.[19] 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.[20] 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.[21] Two years later, concerned members of the House of Representatives held a hearing[22] 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.[23]

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/freedom-net-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-dhs-monitoring-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-v-dhs-media-monitoring/.

the U.S.[24] 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.[25] 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."[26]

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.[27] 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.[28] 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.
[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-reporter-homeland-security-tried-to-take-my-phones-at-the-border.

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.[29] In so holding, the courts noted the significant privacy implications of cloud computing.[30] 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."[31] 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."[32]

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."[33] 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.[34]

---

[29] 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).

[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."

* * *

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