U.S. Customs and Border Protection
Attn: CBP PRA Officer
Office of Trade, Regulations and Rulings,
Economic Impact Analysis Branch
10th Floor, 90 K St NE.
Washington, DC 20229-1177

Re: Comments re OMB Control Number 1651-0139

To Whom It May Concern:

The undersigned groups, a broad range of civil rights, civil liberties, and community organizations, write to express our concerns regarding U.S. Customs and Border Protection's ("CBP") proposal to collect social media identifiers of Chinese visa holders via its Electronic Visa Update System (EVUS), and to demand that CBP withdraw this proposal.

CBP's proposed change would involve collecting "social media identifiers" from B-1, B-2, and B-1/B-2 visa holders from the People's Republic of China for "vetting purposes" via EVUS.[1] We believe that this new proposal would lead to increased profiling based on race and national origin, erode Internet freedom and individual privacy, and ultimately would be an ineffective use of CBP resources.

I. THIS PROPOSAL WOULD LEAD TO INCREASED PROFILING BASED ON RACE AND NATIONAL ORIGIN.

CPB's proposal singles out visitors from China for heightened information collection and scrutiny by U.S. border agents. Visitors from other countries permitted to enter the U.S. on long term B-1, B-2, and B-1/B-2 visas would not be subjected to this rule change. In addition, U.S. citizens and green card holders with family members and associates in China would be affected, as their information could be gathered from targeted visitors' connections and social networks.

The broader context around this proposal is telling. President Trump's intentions to discriminately target China as a threat are well-documented. He has publicly proclaimed China to be an economic enemy of the U.S.; accused China of being "grand champions at manipulation of currency,"[2] going so far as to say the U.S. "can't continue to allow China to rape our country;" and to blame China for engaging in the "greatest theft in the world."[3] Context is directly

[1] A Notice by the U.S. Customs and Border Protection on 02/21/2017, 82 FR 11237 (February 21, 2007), available at https://www.federalregister.gov/documents/2017/02/21/2017-03343/agency-information-collection-activities-electronic-visa-update-system.
[2] Steve Holland and David Lawder, "Exclusive: Trump calls Chinese 'grand champions' of currency manipulation," *Reuters*, (Feb 24, 2017), available at http://www.reuters.com/article/us-usa-trump-china-currency-exclusive-idUSKBN1622PJ.
[3] Candace Smith, "Donald Trump Calls China's Trade Practice the 'Greatest Theft in the World,'" *ABC News*, (May 2, 2016), available at http://abcnews.go.com/Politics/donald-trump-calls-chinas-trade-practices-greatest-theft/story?id=38812125.

relevant; indeed, the courts have long held that they may not "turn a blind eye to the context in which [a] policy arose."[4]

Moreover, this policy fits into a larger historical context of discrimination. The U.S. government's efforts past and present have subjected individuals of Chinese origin to overbroad profiling and targeting as economic and national security threats. From the Chinese Exclusion Act of 1882 banning Chinese immigration, to FBI harassment and surveillance of Chinese Americans during the McCarthy era,[5] to the unjust prosecution and solitary confinement of Wen Ho Lee and recent wrongful prosecutions of Xiaoxing Xi, Sherry Chen, Guoqing Cao, Shuyu Li with false espionage charges,[6] such profiling in the past has had detrimental impacts for individuals while not advancing our national security or safety.

We have also seen another group that has been labeled wholesale as a national security concern, Muslim Americans and visitors from Muslim majority countries, being targeted for invasive and discriminatory social media checks at the U.S. border.[7] Reports have emerged of CBP demanding social media handles and accessing social media posts of Muslim travelers, and even choking a Muslim American citizen after he declined to hand over his phone for inspection.[8] Secretary of Homeland Security John Kelly made his Department's intentions clear for escalating social media scrutiny for refugees and visitors from seven Muslim majority countries when he stated, "[w]e want to get their social media, with passwords—what you do, what you say [and]… [i]f you don't cooperate then you don't come in."[9]

CBP's proposal would result in everyday travelers being treated as more suspect based solely on their race and national origin. This discriminatory policy would only fan the flames of anti-China and anti-Asian sentiment in the U.S., which is already on the rise[10] in conjunction with President Trump's statements throughout his campaign and since taking office. The bottom line is that race-based targeting has never been and will never be an effective national security tool.

II. THIS PROPOSAL WOULD ERODE INTERNET FREEDOM AND INDIVIDUAL PRIVACY

---

[4] *State of Hawai'i and Ismail Elshikh v. Trump et al.*, No. Cv. No. 17-0050 DKW-KSC, Order at 32, (D.Ct HW), quoting McCreary County v. ACLU of Ky, 545 U.S. 844 (2005).

[5] Jonathan H. X. Lee, Chinese Americans: The History and Culture of a People, at 211-212.

[6] These American scientists were all falsely accused by the U.S. government of spying for China. See e.g. Mara Hvistendahl, "Chinese-American scientists in the crosshairs," *Science Magazine*, (Nov 12, 2015), available at http://www.sciencemag.org/news/2015/11/feature-chinese-american-scientists-crosshairs.

[7] David Z. Morris, "Border Agents Reportedly Using Facebook to Screen Travelers Blocked by Trump Order," *Fortune*, (Jan 28, 2017), available at http://fortune.com/2017/01/28/trump-ban-facebook-screening/.

[8] Murtaza Hussain, "Complaints Describe Border Agents Interrogating Muslim Americans, Asking for Social Media Account," *The Intercept*, (Jan 14, 2017), https://theintercept.com/2017/01/14/complaints-describes-border-agents-interrogating-muslim-americans-asking-for-social-media-accounts/.

[9] Olivia Solon, "US border agents could make refugees and visa holders give social media logins," *The Guardian*, (Feb 8, 2017), available at https://www.theguardian.com/us-news/2017/feb/08/border-security-facebook-password-trump-travel-ban.

[10] Advancing Justice-LA, "Significant Increase in Number of Anti-Chinese and Anti-Muslim Hate Crimes in Los Angeles County in 2015," Sept. 29, 2016, *available at* http://advancingjustice-la.org/media-and-publications/press-releases/significant-increase-number-anti-chinese-and-anti-muslim-hate#.WNPzVrGZO1s.

A. Collecting information associated with visitors' "online presence" is highly invasive

An individual's social media identifiers can provide access to an immense amount of sensitive personal information, and this proposal could result in a level of information collection far beyond what is currently required for EVUS enrollment. In having access to an individuals' online presence, border agents could, without individualized suspicion, potentially search for and collect information about visitors' political and religious views and affiliations, professional activities, personal interests, reading lists, location history, and much more. Because social media is highly reliant on social connections, this proposal could also lead to information collection on visitors' family members, friends, colleagues, and other associates, many of whom may be Americans. There is a vast amount of information about an individual's private life that can be obtained through public social media identifiers, unlike in a physical search that is limited by physical constraints. Thus implementing this proposal, or any suspicionless collection of social media information regardless of whether or not it is deemed voluntary, poses a significant threat to individual privacy.

B. Under this proposed policy, there are no protections to prevent misjudgment of visitors' social media activity

Social media posts and connections are very context-, language-, and culture-specific, and the meaning of content is often highly idiosyncratic. The intent and meaning of social media content can be difficult to discern and easily misinterpreted.

In CBP's proposal, there are no standards or guidelines around how social media information would be evaluated or used. In other words, there are no protections to prevent collected social media information from being misjudged, stereotyped, or misconstrued to bar Chinese visitors from traveling to or entering the U.S. This type of misjudgment has already happened in the past—two British tourists were detained and deported at the U.S. border for making a joke on Twitter to "destroy America."[11] The tourists had intended to express having a good time while on vacation in the U.S. using colloquial language that is common in Britain, but their language was mistakenly interpreted as a threat.

Importantly, there is no opportunity for individuals to challenge, explain, or review information about their online presence that is collected if it is taken out of context and used against them. This puts an unfair and undue burden on travelers and their associates and gives CBP agents an undue amount of discretion. Because the proposal provides no guidelines on how to interpret social media information, it could lead to a wide variation of enforcement. An overabundance of discretion from individual CBP agents and lack of uniform standards under this policy stands to violate the principle that immigration laws of the United States should be enforced uniformly.[12] There is also no transparency into how this data would be retained, re-used, or applied for further

[11] Elizabeth Flock, "Twitter joke to 'destroy America' gets two Brits deported from U.S.," *Washington Post*, (Jan 30, 2012), available at https://www.washingtonpost.com/blogs/blogpost/post/twitter-joke-to-destroy-america-gets-two-brits-deported-from-us/2012/01/30/gIQAD0tfcQ_blog.html.
[12] State of Washington et al v. Trump, No. C17-0141JLR, TRO at 6.

investigation or intelligence gathering, so any mistake or misinterpretation of such information could continue to negatively affect travelers over time.

C. Collection of social media information will create a chilling effect on free speech, Internet freedom, and individual privacy

Soliciting social media identifiers from individuals would infringe on freedom of speech and Internet freedom. Nowadays, much of our lives are digital and can be accessed online. We rely on the Internet to stay in touch with friends and family, conduct professional work and personal finances, practicing our faith, and more. Given the intrusive nature of social media collection and the considerable risks for providing this personal information, there would inevitably be a chilling effect around individuals' free Internet expression. Because there could be severe consequences for everyday Internet expression, as seen in the example of the two British tourists, visitors from China and around the world might be prompted to censor their behavior and expressions when coming to the U.S.

Asking for social media identifiers in connection with individuals' passport-verified identities also poses a severe threat to online anonymity. Many individuals, such as Chinese democracy and human rights activists, rely on anonymous online identities to further their activism in a manner that provides some protection from government reprisals. Given the risks and lack of transparency around how CPB will collect and share this information, individuals who remain anonymous or use pseudonyms on social media might suffer severe consequences if their true identities are not guarded and are linked to their social media accounts.

Our country has long advocated for free Internet expression around the world, and this proposed policy serves to erode it. In 2006, then-Secretary of State Condoleezza Rice established the "Global Internet Freedom Task Force" as a U.S. foreign policy initiative to promote Internet freedom abroad; this was in large part a response to foreign governments' repression and censorship. The subsequent administration continued these efforts.[13] In announcing the task force in 2006, Under Secretary of State Josette Shiner said it would address "very serious concerns about the protection of privacy and data throughout the Internet globally and, in particular, some of the recent cases raised in China." China was cited specifically a "serious area of concern" for its repressive privacy practices.[14] Yet here, CBP is proposing to monitor Internet expression of individuals from China, the very country the U.S. has criticized for doing the same.

D. This proposal would have a negative impact for U.S. citizens' civil liberties and business interests abroad due to potential for reciprocity

If this proposal were implemented, it would create a significant possibility for reciprocity—as the U.S. government increases its scrutiny of foreign visitors, foreign governments can do the same for U.S. visitors. This prospect would pose significant risks for U.S. travelers to China,

---

[13] Patricia Moloney Figliola, Casey L. Addis, and Thomas Lum, Congressional Research Service, "U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology," (Jan 3, 2011), *available at* https://fas.org/sgp/crs/row/R41120.pdf.

[14] Carol Walker, "Secretary of State Establishes Global Internet Freedom Task Force," U.S. Embassy Montevideo Archives, (Feb 2006), *available at* http://archives.uruguay.usembassy.gov/usaweb/paginas/2006/06-055EN.shtml.

who could in turn be subjected to information collection by the Chinese government. For the same reasons as mentioned above, if the Chinese government gained access to U.S. citizens' social media information, it could have significant negative civil liberties consequences for U.S. travelers. Furthermore, foreign governments may well be emboldened to take this reciprocity a step further and demand access to Americans' private communications. It would of course be highly detrimental to U.S. economic interests and trade secrets protection abroad if foreign governments could access sensitive online information from U.S. citizens, such as their work-related communications, as they travel abroad for personal or professional purposes. In putting forth a policy like this, it is necessary to consider the possible repercussions around reciprocation, which would be very damaging to the U.S.

III. ULTIMATELY, THIS PROPOSAL WOULD BE INEFFECTIVE FOR PROTECTING NATIONAL SECURITY WHILE CREATING SIGNIFICANT AND UNNECESSARY BURDENS FOR CBP

CBP's proposal implies that soliciting individuals' online identifiers would advance EVUS's goal of protecting the United States' public safety and national security. This premise is misguided, as it assumes individuals who pose a public safety or national security risk would self-disclose their social media information. Individuals who pose a threat could easily provide "dummy" social media profiles to evade or thwart such collection efforts. This program would also likely yield many more replies from travelers who pose no threat, which would waste time and resources and clog our information systems with useless data.

Additionally, processing social media information is very time and resource consuming. Beyond collecting information, interpreting content and contacts would be complex and intensive, and most of the information would not be relevant to security. This would create a large burden for CBP for minimal gains, if any. Thus, in addition to its adverse impact on travelers, this proposal is neither necessary nor does it provide substantive utility to CBP's efforts around security; in fact, it arguably does much to hinder our security.

In conclusion, our organizations recommend that CBP withdraw its proposal to collect social media identifiers of Chinese B-1, B-2, and B-1/B-2 visa holders via EVUS. This proposal would lead to unfettered national origin-based profiling of visitors to the U.S., and would undermine individual privacy and free Internet expression both domestically and abroad. While this proposal is meant to protect national security, it would be ineffective in achieving this purpose.

Sincerely,

Asian Americans Advancing Justice

18millionrising.org

Access Now

Alvaro Bedoya, Center on Privacy & Technology at Georgetown Law

American Civil Liberties Union

Asian American Federation of Florida - South Region

Asian American Legal Defense and Education Fund (AALDEF)

Asian American Organizing Project

Asian Americans United

Asian Law Alliance

Asian Pacific Community in Action

Asian Services In Action, Inc.

CAAAV Organizing Asian Communities

Center for Constitutional Rights

Center for Democracy & Technology

Chinese for Affirmative Action

Chinese Progressive Association

Council on American Islamic Relations - California

Defending Rights & Dissent

Demand Progress

Electronic Frontier Foundation

Emerge-USA

Filipino Advocates for Justice

Florida Chinese Federation

MPower Change

Muslim Public Affairs Council

NANAY CEDC

NANAY, Inc.

National Immigration Law Center

National Lawyers Guild – San Francisco Bay Area Chapter

National Tongan American Society

New Mexico Asian Family Center

OCA – Asian Pacific American Advocates

OCA Greater Houston

OCA South Florida Chapter