



Advisory Board  
Hon. John Burton  
Hon. Nancy Pelosi  
Hon. Cruz Reynoso

Board of Directors  
Cynthia Alvarez  
Richard Boswell  
W. Hardy Callcott  
Eva Grove  
Bill Ong Hing  
Lisa P. Lindelef  
Anita I. Martinez  
Michelle Mercer  
Toni Rembe  
Rudy Ruano  
Guadalupe Siordia-Ortiz  
Lisa Spiegel  
Reginald D. Steer  
Alan Tafapolsky  
Mawuena Tendar  
Hon. James L. Warren  
(Ret.)  
Allen S. Weiner  
Roger Wu

General Counsel  
Bill Ong Hing

Of Counsel  
Don Ungar

Executive Director  
Eric Cohen

**San Francisco**  
1663 Mission Street  
Suite 602  
San Francisco, CA 94103  
t: 415.255.9499  
f: 415.255.9792

**Washington D.C.**  
1016 16<sup>th</sup> Street, NW  
Suite 100  
Washington, DC 20036  
t: 202.777.8999  
f: 202.293.2849

Electronically Submitted to via [Regulations.gov](http://www.regulations.gov)

August 22, 2016

Paperwork Reduction Act Officer  
U.S. Customs and Border Protection  
U.S. Department of Homeland Security  
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; (June 23, 2016); Docket No. 2016-14848; OMB Control Number 1651-0111.**

Dear Paperwork Reduction Act Officer:

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.

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 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) (3<sup>rd</sup> 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>.

*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.

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 intrusion into the private and intimate life of individuals.

---

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

<sup>4</sup> 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>.

<sup>5</sup> 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/>.

<sup>6</sup> *Id.*

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

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.

---

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

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

<sup>9</sup> *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>.

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

<sup>11</sup> 357 U.S. 449, 461 (1958).

## **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.

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.

---

<sup>12</sup> 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/>.

<sup>13</sup> 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).

### 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.

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

---

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

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

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

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

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

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



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.

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

---

<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).

<sup>22</sup> 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/>.

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

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>

## **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

---

<sup>24</sup> 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>.

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*

<sup>27</sup> 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/>.

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



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.

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,

A handwritten signature in black ink, appearing to read 'Jose Magana-Salgado', with a horizontal line extending to the right.

Jose Magana-Salgado  
Managing Policy Attorney  
Immigrant Legal Resource Center