CENTER FOR DEMOCRACY & TECHNOLOGY

November 4, 2019

Department of Homeland Security

Re: Agency Information Collection Activities: Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms (Docket Number DHS-2019-0044)

The Center for Democracy & Technology[1] appreciates the opportunity to provide comments to the Department of Homeland Security (DHS) regarding proposed rule Docket Number DHS-2019-0044.[2] The proposed rule would change two Customs and Border Protection (CBP) applications, Electronic System for Travel Authorization (ESTA) and Electronic Visa Update System (EVUS), by effectively requiring travelers to disclose their social media identifiers. Currently, such disclosure is optional. Additionally, the applications for a number of immigration benefits assessed by United States Citizenship and Immigration Services (USCIS) will now include a demand for disclosure of social media identifiers. This information will be demanded of Lawful Permanent Residents seeking to naturalize (Form N-400), from people applying for political asylum (Form I–589), and many other immigration benefits. Applicants are admonished that "failure to provide the requested data may either delay or make it impossible for CBP to determine an individual's eligibility for the requested benefit" and "failure to provide the requested data may either delay or make it impossible for USCIS to determine an individual's eligibility for the requested benefit."[3] Therefore, the information is functionally required.

We vehemently oppose the mass collection of social media identifiers and implore DHS to revoke this rule. This proposal is spectacularly harmful to the exercise of fundamental rights, and relative to the associated costs to rights, fails to deliver adequately on added security. We have separately joined comments in response to this rule highlighting the attendant problems.[4] In short, this collection will chill freedom of speech and association, inhibit anonymous speech, leave individuals vulnerable to ideological and racial discrimination, and overwhelm the government with irrelevant information. Furthermore, the collection of this data from individuals who will reside in the United States long term, or become citizens, divides our society into two categories of speakers: those about whom the government has a registry of online handles and those about whom the government does not have an online identifier. The introduction of social media screening facilitated by this collection to make decisions about

[1] The Center for Democracy & Technology is a 501(c)(3) organization that advocates for global online civil liberties and human rights. CDT drives policy outcomes that keep the internet open, innovative, and free. The organization supports laws, corporate policies, and technology tools that protect privacy, and advocates for stronger legal controls on government surveillance. https://cdt.org/about/.

[2] Dep't of Homeland Sec., Notice for Request for Comment on Agency Information Collection Activities: Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms (84 Fed. Reg. 46557–46561) Regulations.gov (Sept. 4, 2019), https://www.regulations.gov/docket?D=DHS-2019-0044.

[3] *Id*. at 46559.

[4] Brennan Center et. al, *Coalition Comment in Response to DHS Proposed Social Media Collection*, Ctr. For Democracy & Tech (Nov. 4, 2019), https://cdt.org/?p=83625.

who can enter, stay, and become a citizen of the United States will have dramatic consequences for immigrants, their loved ones, and for our society. CDT has highlighted these harms countless times.[5]

We oppose the adoption of social media screening, but the appetite for this data does not appear to be waning. We proceed below with some initial thoughts on how DHS could diminish some of the adverse impacts of social media screening if it moves forward with this regulation despite widespread opposition.

If DHS Proceeds With This Proposed Collection, The Department Must Take Steps To Mitigate The Predictable Negative Consequences.

DHS has received countless warnings about the predictable negative consequences of social media screening. We have produced a few recommendations that may mitigate *some* of the expected harms. We would welcome a conversation about these initial proposed safeguards, and about additional safeguards that could be put in place.

1. The collection and screening of social media data should be predicated on demonstrated efficacy.

The proposed rule states that agencies have determined that the information sought will aid in the identification and vetting of applicants. This cursory conclusion is inconsistent with other public information calling into question the efficacy of the use of social media information to screen non-citizens.

---

[5] *See, e.g.*, Center for Democracy & Technology, *Comments to DHS Regarding Agency Information Collection Activities: Electronic Visa Update System,* Ctr. For Democracy & Tech (April 24, 2017), https://cdt.org/files/2017/05/CDT-Comments-to-EVUS-Social-Media-Identifier-Proposal.pdf; Center for Democracy & Technology, *Comments to DHS Regarding Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization,* Ctr. For Democracy & Tech (Aug.19, 2016), https://cdt.org/files/2016/08/CDT-comments-DHS-social-media-identifier-proposal.pdf; Center for Democracy & Technology, C*omments to the State Department regarding DS-160 and DS-156, Application for Nonimmigrant Visa, OMB Control No. 1405-0182; DS-260, Electronic Application for Immigrant Visa and Alien Registration, OMB Control No. 1405-185*, Ctr. For Democracy & Tech (May 9, 2018), https://cdt.org/files/2018/05/CDT-Comment-State-Department-Information-Collection.pdf; Center for Democracy & Technology, *Comments to OMB Department regarding DS-160 and DS-156, Application for Nonimmigrant Visa, OMB Control No. 1405-0182; DS-260, Electronic Application for Immigrant Visa and Alien Registration, OMB Control No. 1405-185,* Ctr. For Democracy & Tech *(Sept. 27, 2018),* https://cdt.org/files/2018/09/CDT-Comment-on-Social-Media-Application-for-Non-Immigrant-Visa.pdf; Center for Democracy & Technology, *Coalition Comment to DHS Regarding Retention of Social Media Information in Alien Files*, Ctr. For Democracy & Tech (Oct. 18, 2017), https://cdt.org/files/2017/10/Coalition-Letter-Opposing-DHS-Social-Media-Retention-.pdf.

Independent and internal evaluations have noted shortcomings with social media monitoring as an effective means of assessing applicant eligibility for benefits. A 2017 report by the DHS Office of the Inspector General examined six social media monitoring programs piloted by DHS. It found that "these pilots, on which DHS plans to base future department-wide use of social media screening, lack criteria for measuring performance to ensure they meet their objectives."[6] DHS has also internally questioned the efficacy of its social media monitoring pilot programs. In a brief from late 2016 prepared for the incoming administration, DHS reported that in three out of its four programs used to vet refugees, "the information in [social media] accounts did not yield clear, articulable links to national security concerns, even for those applicants who were found to pose a potential national security threat based on other security screening results."[7] DHS also noted that it was difficult to discern the "authenticity, veracity, [and] social context," of social media content, as well as "whether the content evidences indicators of fraud, public safety, or national security concern."[8] DHS officials concluded that "mass social media screening" was a poor use of resources: "[t]he process of social media screening and vetting necessitates a labor intensive manual review," taking people away from "the more targeted enhanced vetting they are well trained and equipped to do."[9]

Furthermore, in 2016, CBP began collecting on a voluntary basis social media identifiers from nationals of countries participating in the Visa Waiver Program, who applied for permission to enter the United States using ESTA. Shortly thereafter, the program was subjected to a Privacy Compliance Review to assess the solicitation and use of social media identifiers.[10] During the review "CBP presented a small sample of success cases, in which the use of social media identifiers significantly aided in the screening and vetting of individuals seeking to travel to the United States."[11] The Privacy Office observed that these anecdotes, "supported the use of social media information in order to assist in determining an individual's eligibility to travel to the United States [], to assist in determining if the applicant posed a law enforcement or security risk, as well as mitigate potentially derogatory information that would likely have resulted in the denial of an individual's ability to travel []."[12] However, CBP did not set up a process to measure how effective social media information was to aiding its work. The Privacy Office recommended that, "CBP [] implement a process or mechanism for tracking and measuring the viability and success of the collection and use of social media information as part

[6] Office of Inspector General, Dep't of Homeland Security, DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success, No. OIG-17-40, 1, (Feb. 27, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.
[7] USCIS Briefing Book, 181, https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf.
[8] *Id.* at 183.
[9] *Id*. at 183-4.
[10] U.S. Dep't of Homeland Sec., Privacy Compliance Review of the U.S. Customs and Border Protection Electronic System for Travel Authorization, (Oct. 27, 2017), https://www.dhs.gov/sites/default/files/publications/CBP-ESTA%20PCR%20final%20report%2020171027.pdf.
[11] *Id*. at 8.
[12] *Id*.

of the screening and vetting process."[13] At the time of the report, CBP was working on creating the technical means to capture this information, and the Privacy Office observed that such data would help assess whether the inclusion of the data is a boon to vetting capabilities or whether it could instead "permit DHS and CBP to determine whether more information is being collected than is necessary to fulfill its specified purposes."[14] The report ends noting that an auditing process was in place, and that the CBP Privacy and Diversity Office would provide a follow up report in 6 months' time addressing the implementation of the recommendations. DHS has not publicly disclosed this report even though its disclosure would help the public assess whether there are adequate processes in place to measure the efficacy of this collection program, and if so, whether the collection is effective.

We urge CBP and USCIS to review existing collection programs to determine whether use of social media data has aided vetting in particular programs as compared to use of other information already available for such vetting. Such an assessment would help the agencies determine whether collecting this information wastes resources, and to determine use limitations that would further the agency's mission but extend some rights protections—for example, turning to social media data only to confirm or refute derogatory information.

2. DHS, CBP, and USCIS must be transparent about the guidance and training provided employees who review social media information.

Given the sensitivity of the data collection, DHS and its agencies must make further efforts to inform the public about the operation of social media screening, and the safeguards in place to preserve rights. This includes making clear who is authorized to review and interrogate social media information. Is any employee permitted to conduct a review? Are CBP border agents permitted? Asylum officers? Will a social media review occur for each application for a benefit? Or, is this information reviewed only for those persons subject to secondary screening processes by select analysts? Armed with this information, civil society would be in a better position to identify defects and recommend safeguards. Furthermore, DHS and its agencies should disclose trainings and guidance provided to personnel on the First Amendment, on social media data quality limitations, and on preserving privacy, civil rights and civil liberties during the operation of social media screening. We acknowledge that some documents have already been made public including the National Vetting Center PIA,[15] CBP's Situational

[13] *Id*. at 3.
[14] *Id*. at 10.
[15] U.S. Dep't of Homeland Sec., DHS/ALL/PIA-072, Privacy Impact Assessment for the National Vetting Center (NVC), (Dec. 11, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall072-nvc-december2018.pdf.

Awareness and Public Social Media Monitoring Initiative PIA,[16] CBP's ESTA PIA,[17] and USCIS's PIA for the Fraud Detection and National Security Directorate.[18] However more must be disclosed, including those materials CDT has requested.[19]

3. DHS must increase protection for First Amendment rights.

A key concern about government social media screening is that much content on social media platforms can reflect one's political and religious beliefs, as well as associational activity. Numerous news stories call into question DHS' commitment to respecting innocent First Amendment-related activity.[20] In May 2019, Acting Secretary of Homeland Security Kevin McAleenan issued a memorandum to all DHS employees regarding the agency's responsibility to adhere to First Amendment protections. The memorandum problematically asserts DHS's authority to maintain a record of how a U.S. citizen or a lawful permanent resident exercises their First Amendment rights.[21] As a result, there is a high risk that social media information reflecting the First Amendment-protected activities of citizens and lawful permanent residents

[16] U.S. Dep't of Homeland Sec., Customs and Border Protection, DHS/CBP/PIA-058, Privacy Impact Assessment for the Publicly Available Social Media Monitoring and Situational Awareness Initiative, (March 25, 2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp58-socialmedia-march2019.pdf.

[17] U.S. Dep't of Homeland Sec., Customs and Border Protection, DHS/CBP/PIA-007(g) Privacy Impact Assessment Update for the Electronic System for Travel Authorization, (September 1, 2016), https://www.dhs.gov/publication/electronic-system-travel-authorization.

[18] U.S. Dep't of Homeland Sec., U.S. Citizenship and Immigration Services, DHS/USCIS/PIA-013-01, Privacy Impact Assessment for the Fraud Detection and National Security Directorate, (Dec. 16, 2014), https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-fdns-november2016_0.pdf.

[19] Center for Democracy & Technology, *CDT FOIA Request to CBP*, (Aug. 14, 2019), https://cdt.org/files/2019/08/CDT-FOIA-CBP-Directive-Operational-Use-of-Social-Media.pdf (requesting CBP Directive 5410-003 – Operational Use of Social Media (Jan. 2, 2015)); Center for Democracy & Technology, *CDT FOIA Request to USCIS*, (Aug. 27, 2019), https://cdt.org/files/2019/08/CDT-FOIA-USCIS-Social-Media-Monitoring-Policies.pdf (requesting USCIS procedures and training focused on understanding data quality limitations associated with social media, USCIS's Operational Use of Social Media, USCIS's Privacy Requirements for the Operational Use of Social Media training, and USCIS "Rules of Behavior" for social media monitoring); Center for Democracy & Technology, *CDT FOIA Request to CBP*, (Sept. 10, 2019), https://cdt.org/files/2019/09/CDT-FOIA-CBP-First-Amendment-and-Social-Media-Training-Materials.pdf (requesting any guidance CBP personnel receive on the treatment of First Amendment protected activity on social media, the social media training provided CBP personnel from the Office of Chief Counsel and the CBP Privacy and Diversity Office).

[20] *See, e.g.,* Tom Jones, Mari Payton & Bill Feather, *Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database*, NBC 7 San Diego (Mar. 6, 2019), https://www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html; Karen Zraick & Mihir Zaveri, *Harvard Student Says He Was Barred From U.S. Over His Friends' Social Media Posts*, N.Y. Times (Aug. 27, 2019), https://www.nytimes.com/2019/08/27/us/harvard-student-ismail-ajjawi.html; Jimmy Tobias, Exclusive: ICE Has Kept Tabs on 'Anti-Trump' Protests in New York City, The Nation (Mar. 6, 2019), https://www.thenation.com/article/ice-immigration-protest-spreadsheet-tracking/.

[21] Memorandum from Kevin McAleenan, to All DHS employees, "Information Regarding First Amendment Protected Activities," Dep't Homeland Sec., (May 17, 2019), https://www.dhs.gov/sites/default/files/publications/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019.pdf.

could be incorporated into applicants' files. DHS should include this information only if absolutely necessary, or if the First Amendment-related conduct is itself the basis of denial. And while not required by the Privacy Act, as a matter of policy DHS should extend this same protection to everyone seeking a decision from DHS, not just U.S persons. By increasing these protections, DHS will be better able to focus on true threats and will be less likely to conflate innocent expressive activity with intent to harm.

4. CBP and USCIS should submit to regularly conducted DHS privacy compliance reviews and internal audits.

We applaud the use of the DHS privacy office to review CBP's ESTA program in 2017. As noted above, more information about the follow up must be disclosed. As USCIS and CBP move forward with social media screening such reviews and subsequent audits should be regularly conducted, the products of which must be made public.

5. Decisions should not be made based solely, or significantly, on social media information.

Social media data is prone to interpretive mistakes. The information is context-dependent and employs forms of communication that are not easily discerned, including slang, emojis, content engagements including reshares and likes, foreign languages, etc. Because it is so easy to get the analysis wrong, decisions should not be based solely, or significantly, on social media information. We acknowledge that in the review of CBP's ESTA program the Privacy Office received confirmation from ESTA and the National Targeting Center that "there [were] no instances in which social media information was the sole factor in an eligibility determination."[22] This should be the rule for all decision-making based in part on social media information. Finally, because social media data is prone to interpretive mistakes, where it is considered in a decision, it should carry little weight relative to other more reliable sources of information.

6. If providing a social media identifier would force an individual to admit to a crime, the collection should be waived.

In some countries, it is a crime to use a social media platform, and in others, the platforms are banned. People may access them by using a Virtual Private Network, but such use to get around the ban can also be a criminal offense.[23] DHS should not put people in the impossible position

[22] U.S. Dep't of Homeland Sec., Privacy Compliance Review of the U.S. Customs and Border Protection Electronic System for Travel Authorization, (Oct.27, 2017), https://www.dhs.gov/sites/default/files/publications/CBP-ESTA%20PCR%20final%20report%2020171027.pdf.

[23] *See, e.g.*, Freedom House, Freedom on the Net 2018, China, https://freedomhouse.org/report/freedom-net/2018/china; Freedom House, Freedom on the Net 2018, Iran, https://freedomhouse.org/report/freedom-

of admitting on paper to committing what constitutes a crime in their home country due to censorship laws. Once collected, the social media information may be shared with other governmental agencies in bulk or on a case-by-case basis, and those agencies may share it with foreign governments. Any adopted restrictions on such sharing will be unknown to the applicant whose social media information is requested. He or she may choose not to use social media in order to avoid the risk that the admission that they use a platform unlawful in their country is learned by their government. Rather than furthering such censorial results in repressive regimes, DHS should make it clear to applicants that admitting to use of social media banned in their country is not required.

7. Making a mistake in the social media data field should not be grounds for denial.

DHS is requesting five years' worth of identifiers from 19 social media platforms, not all of which are still operational.[24] The regulation contemplates that this list will add and subtract platforms as they come on-line or become defunct. It is not reasonable to expect an applicant to remember all of the social media platforms they have used in the last five years. A report in 2017 found that the average person has 7.6 active social media accounts, with the number rising to 8.7 for those aged 16-34.[25] Applicants may temporarily create an exploratory account to try a new social media platform before deciding whether to create an account they would use more permanently. Moreover, longevity is the exception in social media networks, not the rule. For example, Vine emerged in 2012 and shut down by 2016.[26] An applicant could have easily created an account on the service and long forgotten about it—but the DHS proposal could expect her to report that account until 2021. Indeed, while platforms may capture the attention of millions at one moment, the wrong update or design could send users running.[27] It is easy to anticipate that applicants will forget to provide social media handles they haven't used for years, or that they set up just to test a service. DHS should establish processes to ensure that such a mistake does not result in denial of a benefit or permission to come to the U.S.

8. Limit use of social media data to corroborating derogatory information.

The proposed regulation is silent as to when investigators or adjudicators are to turn to a review of an applicant's public social media data. In order to avoid some of the pitfalls we warn

---

net/2018/iran; *10 Most Censored Countries*, Committee to Protect Journalists, https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist.php (last accessed Nov. 4, 2019).

[24] ASK FM; DOUBAN; FACEBOOK; FLICKR; INSTAGRAM; LINKEDIN; MYSPACE; PINTEREST; QZONE (QQ); REDDIT; SINA WEIBO; TENCENT WEIBO; TUMBLER; TWITTER; TWOO; VINE; VKONTAKTE (VK).

[25] *See* Colm Hebblethwaite, The average person has 7 social media accounts, Marketing Tech News (Nov. 17, 2017), https://www.marketingtechnews.net/news/2017/nov/17/average-person-has-7-social-media-accounts/.

[26] *See* Catherine Rowell, The rise and fall of Vine: A brief timeline, Business Chief (Oct. 28, 2016), https://www.businesschief.com/technology/5614/The-rise-and-fall-of-Vine:-A-brief-timeline.

[27] *See* Kaya Yurieff & Seth Fiegerman, Snapchat user growth stagnant amid redesign backlash, CNN (May 1, 2018), http://money.cnn.com/2018/05/01/technology/snapchat-user-growth-redesign/index.html.

about, if it is to be reviewed, social media data should be turned to only when there is existing derogatory information in the application that warrants a closer review of an application. Using social media information on the front end of a decision-making process would waste resources, delay adjudications, and leave applicants vulnerable to a fishing expedition that may result in a denial because an analyst inappropriately disfavored them. The DHS Privacy Office review noted that there were some cases where the collection of social media data mitigated derogatory information about an applicant.[28] We think the use, if any, of social media information should be left to these secondary reviews.

9. There must be a right to refute or explain information.

Judgments made based on social media information should be properly documented and made available to the applicant so that the applicant has an opportunity to refute. This includes both the social media data itself and the judgments drawn from the review of the data. Regardless of whether this should be the case for all derogatory information, social media information is particularly vulnerable to mistaken inferences.

10. Applicants must not be held accountable for the speech of others.

Individuals should not be held responsible for the speech of others online. For example, earlier this year a Palestinian student who was admitted to Harvard University was interrogated about the speech of a social media friend—speech with which he did not engage—and was initially denied entry to the U.S.[29] While this erroneous decision was ultimately reversed, permitting decisions to be based on what others say will cause applicants to severely limit their online engagements.

11. Social media information should be subject to limited retention periods.

A major concern is that the U.S. government will retain social media identifiers and any collected content from profiles far longer than is truly necessary. This information is sensitive. Many speak on the condition of anonymity because they fear reprisal; many are not allowed to use the platforms and must do so discreetly. DHS should consider not retaining this information beyond the initial grant of a benefit, or no longer than an individual has permission to stay in the United States. Data disposal should be the instinct.

---

[28] U.S. Dep't of Homeland Sec., Privacy Compliance Review of the U.S. Customs and Border Protection Electronic System for Travel Authorization, 7 (Oct. 27, 2017), https://www.dhs.gov/sites/default/files/publications/CBP-ESTA PCR final report 20171027.pdf.

[29] Karen Zraick & Mihir Zaveri, *Harvard Student Says He Was Barred From U.S. Over His Friends' Social Media Posts*, N.Y. Times (Aug. 27, 2019), https://www.nytimes.com/2019/08/27/us/harvard-student-ismail-ajjawi.html; Mana Azarmi, Ismail Ajjawi's Fundamental Free Speech & Association Rights Trampled by U.S. Customs and Border Protection, Ctr. For Democracy & Tech, (Aug. 28, 2019), https://cdt.org/blog/ismail-ajjawis-fundamental-free-speech-association-rights-trampled-by-u-s-customs-and-border-protection/.

Individuals applying for a benefit before USCIS currently face indefinite retention of social media data: the data is stored in their Alien File, the retention period for which is 100 years after an individual's birth date, after which the data is sent to the National Archives and Records Administration for permanent retention.[30] Indefinite retention of information poses a particularly significant problem for lawful permanent residents and naturalized citizens. The government's retention of their social media identifiers, and any associated content of their speech, will have long term chilling effects on these populations. The existence of a persistent dossier of a naturalized citizen's social media activity will mean that these citizens face scrutiny of the record of their past social media activity in ways that U.S.-born citizens will not routinely face. The solution is to delete this data from Alien Files once an individual has been granted a green card, or at the very least once they have naturalized.

12. Speech critical of the United States is likely not relevant to an eligibility determination. Avoid questioning it.

The U.S. government should not be in the business of excluding people merely because they criticize the U.S. government, or its allies. Criticism of U.S. policies generally is irrelevant to the criteria that establish admissibility or eligibility for an immigration benefit. A focus on critical speech can detract from focusing on true threats, and is the kind of activity that censors vibrant online debate.

13. DHS, CBP, and USCIS should not adopt faulty automated predictive tools to screen applicants.

Given the volume of information the government will be collecting there will be a temptation to use algorithms to screen for information indicative of a threat to the United States. We strongly caution DHS against adopting tools that claim to offer predictive judgments about applicants, similar to the kind desired by Immigration and Customs Enforcement in 2017.[31] Immigration and Customs Enforcement (ICE) explored establishing an automated vetting system that would input applicants' social media data into predictive machine-learning models to generate investigative leads, in a proposal known as "Visa Lifecycle Vetting" (formerly "Extreme Vetting").[32] In the case of ICE's Visa Lifecycle Vetting plan, the criteria ICE sought to predict were amorphous and undefined, leading 54 of the nation's leading computer science experts to send a letter to DHS, stating that "no computational methods can provide reliable or objective assessments of the traits that ICE seeks to measure."[33] Furthermore, as CDT has explained in a

[30] Dep't of Homeland Sec., Notice for Request for Comment on Privacy Act of 1974; System of Records (82 Fed. Reg. 43556) (Sept. 18, 2017), https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records.

[31] Natasha Duarte, *ICE Finds Out It Can't Automate Immigration Vetting. Now What?*, Ctr. For Democracy & Tech. (May 22, 2018), https://cdt.org/blog/ice-cant-automate-immigration-vetting/.

[32] See ICE-HSI, "Extreme Vetting Initiative: STATEMENT OF OBJECTIVES (SOO)," June 12, 2017, FedBizOpps.Gov.

[33] Center for Constitutional Rights, Coalition Letter to DHS Opposing Extreme Vetting Initiative (Nov. 16, 2017), https://ccrjustice.org/coalition-letter-dhs-opposing-extreme-vetting-initiative.

white paper, automated tools for analyzing the text of social media posts cannot reliably interpret the meaning of a post or the speaker's intent.[34] DHS and its agencies should steer clear of these tools.

14. DHS, CBP, and USCIS must consult with civil society and affected populations about the impact of this collection.

If the agencies move forward with social media screening DHS, CBP, and USCIS should convene meetings with civil society, as well as affected populations to understand what affect the collection of social media identifiers, and any associated screening is having on the exercise of rights. Such convenings could alert the agencies to the need to invest more resources in ensuring that analysts have the cultural competency needed to understand the social media content they are reviewing. They could also alert the agencies to the gravity of the harms caused.

* * *

CDT strongly opposes this collection and urges DHS to revoke this proposed rule. As more of our discourse migrates online, this proposal risks great harm to the exercise of fundamental rights and to the health of our democracy. In the event the rule goes forward, we urge DHS to consider these initial thoughts on how it can mitigate some harms. We welcome questions regarding these recommendations. *(Please direct any response to these recommendations to CDT Policy Counsel Mana Azarmi, mazarmi@cdt.org.)*

[34] Natasha Duarte, Emma Llanso & Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis*, Ctr. For Democracy & Tech. (Nov. 2017), https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf.