

September 15th, 2021

The Honorable Alejandro Mayorkas  
Secretary of Homeland Security  
United States Department of Homeland Security  
2707 Martin Luther King Jr Ave SE  
Washington, DC 20528

Dear Secretary Mayorkas,

Our coalition of civil libertarians, technologists, and advocates for government accountability and civil and human rights thanks you for meeting with us to discuss our concerns associated with select Department of Homeland Security (DHS) programs. We appreciate your considering policy solutions to mitigate these concerns. Although not all of our organizations work directly on—or can speak directly to—all of the recommendations described below, we write to you jointly to summarize the key concerns we raised at the meeting and the recommendations we offered to address them.

As you noted, the Department’s “welcome” is the first interaction that virtually all migrants and visitors to the United States receive. We want to ensure that sentiment applies to the civil rights and liberties of citizens and non-citizens alike, at the border and throughout the country. Our key recommendations for the Department will help ensure it can perform its missions while respecting civil rights and civil liberties and creating a welcoming and inclusive atmosphere.

To that end, we have two overarching requests, and three requests concerning specific programs.

- First, we ask that you review and revise the Department’s non-discrimination and racial profiling guidance, including DHS’s 2013 memorandum on the Department’s Commitment to Nondiscriminatory Law Enforcement and Screening Activities and CBP’s 2020 Policy on Nondiscrimination in Law Enforcement Activities and All Other Administered Programs.<sup>1</sup> These materials, taken together with the Department of Justice’s 2014 racial profiling guidance,<sup>2</sup> permit bias-based profiling in the national security context, at the border, and in protective, inspection, or screening activities. They further facilitate abusive approaches across a range of Department policies, programs, and subcomponents.<sup>3</sup> New guidance

---

<sup>1</sup> Memorandum from Sec’y Napolitano, Dep’t of Homeland Sec., to Component Heads (Apr. 26, 2013), [https://www.dhs.gov/sites/default/files/publications/secretary-memo-race-neutrality-2013\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/secretary-memo-race-neutrality-2013_0.pdf); *CBP Policy on Nondiscrimination in Law Enforcement Activities and all other Administered Programs*, Dep’t of Homeland Sec. (last modified Feb. 24, 2020), <https://www.cbp.gov/about/eo-diversity/policies/nondiscrimination-law-enforcement-activities-and-all-other-administered>.

<sup>2</sup> See *Fact Sheet: U.S. Department of Justice Racial Profiling Guidance*, Dep’t of Homeland Sec. (Dec. 8, 2014), <https://www.dhs.gov/news/2014/12/08/fact-sheet-us-department-justice-racial-profiling-guidance>; Dep’t of Justice, *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation or Gender Identity* (Dec. 2014), [https://www.dhs.gov/sites/default/files/publications/use-of-race-policy\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/use-of-race-policy_0.pdf).

<sup>3</sup> The Department adopted the policy after insisting that it was “impractical to ignore ethnicity when it came to border enforcement.” See Matt Apuzzo & Michael S. Schmidt, *U.S. to Continue Racial, Ethnic Profiling in Border Policy*, N.Y. Times (Dec. 5, 2014), <https://www.nytimes.com/2014/12/06/us/politics/obama-to->

should explicitly prohibit profiling based on actual or perceived race, religion, national origin, sexual orientation, or gender (including gender identity and expression), without any exceptions.

- Second, we ask you to order the Department to map and make public (1) the various kinds of information collected by the Department, (2) the legal authority for collection and retention,<sup>4</sup> (3) the purposes for which it is used, (4) how it flows within the Department and to other agencies and foreign governments, and (5) the impact of that collection, retention, and sharing on civil rights and liberties. As former DHS officials have asserted, the Department’s collection and use of information about citizens and people traveling to or living in this country raise such significant concerns that “the privacy and due process concerns resulting from other homeland security operations, such as information collection by the National Security Agency, pale by comparison.”<sup>5</sup> Yet there is almost total opacity about what information is collected and how it is used. Privacy Impact Assessments are important, but not enough, as they can be program-specific, or concern only parts or phases of programs. Without this kind of mapping, Congressional oversight and public accountability are extremely difficult if not impossible.

We also urge you to direct the Office of Civil Rights and Civil Liberties (CRCL) to conduct a thorough review of the DHS programs below, and to empower it to recommend termination of programs when appropriate. In our view such a review should focus, at minimum, on the following key areas:

1. Reviewing the Department’s widespread surveillance and use of social media;
2. Assessing DHS’s purchase and collection of data from third parties; and
3. Critically evaluating the Department’s programs that claim to predict or prevent violence including domestic terrorism.

The results of such reviews should be made publicly available, in redacted form if necessary.

In addition to these reviews, we urge DHS to adopt the privacy reforms described below.

---

[impose-racial-profiling-curbs-with-exceptions.html](#). For example, a March 2021 ACLU report examining Border Patrol activities in Michigan found evidence of rampant profiling: over 96% of people arrested by the Border Patrol’s Detroit Sector were recorded as being “Black,” “Dark Brown,” “Dark,” “Light Brown,” “Medium Brown,” “Medium,” or “Yellow.” ACLU of Mich., *The Border’s Long Shadow: How Border Patrol Uses Racial Profiling and Local and State Police to Target and Instill Fear in Michigan’s Immigrant Communities* 4 (Mar. 2021), [https://www.aclumich.org/sites/default/files/field\\_documents/100\\_mile\\_zone\\_report\\_updated.pdf](https://www.aclumich.org/sites/default/files/field_documents/100_mile_zone_report_updated.pdf).

<sup>4</sup> Chappell Lawson & Alan Douglas Bersin, *Beyond 9/11: Homeland Security for the Twenty-First Century* 303 (Chappell Lawson et al., eds., 2020), <https://mitpress.mit.edu/books/beyond-911> (noting that DHS relies on “implied consent” to justify the retention of “huge amounts of data on individuals”).

<sup>5</sup> *Id.* (“[DHS] is the only government entity that, as part of its regular operations, conducts invasive physical searches of millions of Americans and their belongings each week without any predicate. It is also one of the only government agencies that retains huge amounts of data on individuals, using only “implied consent” for justification. In addition, it draws inferences based on data in ways that are totally opaque to citizens, and takes actions that may be to their individual detriment (being selected for search and interrogation, being delayed or severely inconvenienced in their travel, etc.). ... [T]he privacy and due process concerns resulting from other homeland security operations, such as information collection by the National Security Agency, pale by comparison.”).

## DHS Collection and Monitoring of Social Media Information

DHS and several of its components engage in the widespread collection of social media identifiers and content. DHS has not demonstrated that these programs are either efficient or necessary. Social media is a challenging field to navigate, especially for a Department that vets visitors who hail from hundreds of countries and speak thousands of languages. In fact, the Office of Information and Regulatory Affairs (OIRA) recently rejected a DHS proposal (first promulgated under then-Acting Secretary McAleenan) to expand dramatically its collection of social media identifiers on travel and immigration forms;<sup>6</sup> OIRA ruled that the Department had not “adequately demonstrated the practical utility of collecting this information.”<sup>7</sup> Nevertheless, CBP continues to request that applicants provide their social media identifiers on Electronic System for Travel Authorization (ESTA) and Electronic Visa Update System (EVUS) applications. We recommend that DHS apply OIRA’s conclusion to these programs as well and halt all collection of social media identifiers through the ESTA and EVUS systems.

Similarly, DHS should terminate its other social media surveillance programs, such as the Visa Lifecycle Vetting Initiative (VLVI), through which ICE uses social media to track visa holders during the entire lifecycle of their interactions with the U.S. government.<sup>8</sup> ICE operates a sister program, the Overstay Lifecycle program, which screens social media from visa applicants for an unspecified amount of time.<sup>9</sup> Pervasive surveillance of this kind has not been shown to be necessary or effective and raises serious First Amendment concerns. In addition to ending these programs, DHS should purge any social media handles, aliases, and other associated identifying information from individuals’ A-Files and from any other DHS databases unless related to criminal activity.

In addition, we note that Presidential Proclamation 10141, President Biden’s proclamation ending the Muslim Ban, directed your office and the Secretary of State, in consultation with the Director of National Intelligence, to conduct a review of the “use of social media identifiers in the screening and

---

<sup>6</sup> See, e.g., Agency Information Collection Activities: Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms, 85 Fed. Reg. 7,563 (Feb. 10, 2020), available at [https://www.reginfo.gov/public/do/PRAViewDocument?ref\\_nbr=202007-1601-001](https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=202007-1601-001).

<sup>7</sup> Notice of Office of Management and Budget Action ICR Reference No. 202007-1601-001, Off. of Info. and Regulatory Affairs (Apr. 2, 2021), [https://www.reginfo.gov/public/do/PRAViewICR?ref\\_nbr=202007-1601-001](https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202007-1601-001).

<sup>8</sup> The contract for ICE’s VLVI was awarded to SRA International (now CSRA Inc., owned by General Dynamics), though the award was initially challenged by two other companies. U.S. Gov’t Accountability Off., GAO B-416734, Decision: Matter of ManTech Advanced Systems International, Inc. (2018), <https://www.gao.gov/assets/b-416734.pdf>; U.S. Gov’t Accountability Off., GAO B-416734.2, Decision: Matter of Amyx, Inc. (2019), <https://www.gao.gov/assets/b-416734.2.pdf>. Both protests were eventually denied by the Government Accountability Office and funding was officially awarded to SRA in May 2019. *Blanket Purchase Agreement (BPA) Call PIID 70CMSD19FC0000020*, Award Profile Contract Summary (May 30, 2019), <https://www.usaspending.gov/award/81011540>. See also McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. Times (Oct. 2, 2019), <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>.

<sup>9</sup> Faiza Patel et al., *Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security*, Brennan Center for Justice 24 (Mar. 11, 2020), <https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf>.

vetting process” and issue a report no later than May 20, 2021.<sup>10</sup> Our understanding is that this review still has not been completed; we request an estimated date by which the review will be complete, and ask your office to commit to releasing a public version.

### Terminate Dagnet Surveillance by DHS and its Contractors

We are deeply concerned about large-scale surveillance and collection of privately held data, whether conducted by DHS or one of its many private sector contractors. In recent years, DHS has secretly scanned the faces<sup>11</sup> of millions of drivers and contracted with companies that secretly and indiscriminately scrape Americans’ photos<sup>12</sup> off of the Internet, track their movements on public roads,<sup>13</sup> and amass vast databases tracking the movements of Americans’ smartphones.<sup>14</sup> DHS also contracts with companies that compile the utility information of over 150 million Americans.<sup>15</sup> Families need gas, water, and electricity to survive, and a phone line for emergencies. Their children need the Internet to attend school. DHS’s use of this data immorally leverages immigrants’ basic needs to target people for deportation.

We urge DHS to immediately end its purchases of sensitive data from third-party vendors and its own dragnet surveillance. In particular, DHS should terminate contracts to purchase people’s cell phone location data, and it should terminate contracts with companies that indiscriminately surveil the public or collect data in violation of state or federal law. The Department should also halt its own suspicionless surveillance; adopt a complete moratorium on its use of face recognition for immigration enforcement; and withdraw its notice of proposed rulemaking to expand CBP’s use of face surveillance at airports and the border. In addition, DHS should prohibit its immigration agents from accessing or collecting electronic records and physical documents derived from essential service providers such as gas, water, electric, phone, and Internet companies.

We further urge DHS to eliminate the near-total secrecy that surrounds its surveillance programs, including use of social media. Specifically, it should regularly brief members of Congress, governors, and key state legislators about the nature and scope of its surveillance activities, and it should issue annual public reporting concerning the same, akin to its annual data mining report and the regular

---

<sup>10</sup> Proclamation No. 10141, 86 Fed. Reg. 7,005 (Jan. 20, 2021), <https://www.federalregister.gov/documents/2021/01/25/2021-01749/ending-discriminatory-bans-on-entry-to-the-united-states>.

<sup>11</sup> Drew Harwell, *FBI, ICE Find State Driver’s License Photos are a Gold Mine for Facial-Recognition Searches*, Wash. Post (July 7, 2019), <https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/>.

<sup>12</sup> Ryan Mac et al., *Clearview’s Facial Recognition App Has Been Used By The Justice Department, ICE, Macy’s, Walmart, And The NBA*, BuzzFeed News (Feb. 27, 2020), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

<sup>13</sup> Vasudha Talla, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations*, ACLU (Mar. 13, 2019), <https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data>.

<sup>14</sup> Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. Journal (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>.

<sup>15</sup> Drew Harwell, *ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations*, Wash. Post (Feb. 26, 2021), <https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/>.

reports from the Offices of Privacy and Civil Rights and Civil Liberties. In addition, as part of its civil rights and civil liberties review, DHS should analyze the privacy and legal implications of its purchases of detailed and highly personal data from third-party vendors and provide public reporting and briefings on those practices as well.<sup>16</sup> As courts apply the Fourth Amendment in novel technological contexts, a fresh legal analysis of these issues is essential. DHS has an opportunity to reaffirm a robust commitment to Americans' privacy and civil liberties in our digital age.<sup>17</sup>

### Suspend DHS Programs that Claim to Predict Fraud, Violence, or Domestic Terrorism

We remain deeply troubled by existing and proposed DHS systems that purport to assess whether an individual poses a “threat” or to predict instances of fraud, violence, or radicalization. At the heart of these systems is the Automated Targeting System (ATS), which relies on secret rule sets and algorithms, in combination with public data such as social media, and can result in prolonged border detention, intrusive searches, and unexplained visa denials. DHS components utilize ATS for programs like ATLAS and Continuous Immigration Vetting (CIV) to identify potential instances of immigration fraud, pursue denaturalization cases, or conduct risk assessments of travelers, among other applications.

Given the well-documented harms of algorithmic bias and concerns that the “rules” these systems use reflect bias as well, we recommend DHS suspend the use of ATS for certain programs that implicate individual rights and liberties, including ATLAS and CIV, pending a thorough review of the civil rights and civil liberties impacts of these systems, including the public release of disparate impact assessments for each such system. We also recommend that DHS conduct a thorough review of the civil rights and civil liberties impact of its use of risk assessments for travelers and publicly release the results.

Finally, we are dismayed that DHS continues to embrace the narrative that it can prevent violence or “domestic terrorism” through social media monitoring or through its Center for Prevention Programs and Partnerships (CP3). We are, of course, concerned about white supremacist violence, but CP3 is grounded in the flawed idea that there is an “evidence-based process” that can reliably identify potential offenders in advance by applying vague indicia of violence, such as a person's views, mental health, or social condition.<sup>18</sup> We know of no credible and independent empirical basis for these claims. Programs grounded in these same assumptions have a long history, but they have never been shown to have stopped someone from becoming a violent extremist and engaging in terrorism. Moreover, these programs are counterproductive and likely to precipitate racial and religious discrimination. Similarly, in the social media monitoring context, DHS appears to be searching for particular “narratives”<sup>19</sup> that may lead to real-world violence, an effort that similarly

---

<sup>16</sup> In addition, DHS should release the existing legal opinions concluding that it may engage in this practice.

<sup>17</sup> See generally, e.g., *Leaders of a Beautiful Struggle v. Baltimore Police*, 2 F.4th 330 (4th Cir. 2021); *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

<sup>18</sup> See Harsha Panduranga, *Community Investment, Not Criminalization: A Call to Abandon the Department of Homeland Security's Violence Prevention Strategy*, Brennan Center for Justice (June 17, 2021), <https://www.brennancenter.org/our-work/research-reports/community-investment-not-criminalization>.

<sup>19</sup> Ken Dilanian, *DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media*, NBC News (May 10, 2021), <https://www.nbcnews.com/politics/national-security/dhs-launches-warning-system-find-domestic-terrorism-threats-public-social-n1266707>.

has no empirically sound premise and will inevitably sweep in large amounts of constitutionally protected speech.<sup>20</sup>

### Empower and Elevate Privacy Office and Office of Civil Rights and Civil Liberties

We conclude by urging you to empower both the Privacy Office and the Office of Civil Rights and Civil Liberties to ensure their prominent and effective role within the Department and with respect to Congress and the public. During our meeting, we appreciated your willingness to emphasize to the Department as a whole the importance of the Privacy Office’s role and work. We believe it is critical for both the Privacy Office and CRCL to have a seat at the table from the point of inception and design of policies and programs that directly impact or implicate civil rights and liberties and privacy—and to ensure that there are benchmarks to measure the effectiveness and impact of programs on communities of color, Muslim communities, and other marginalized communities before programs are launched.

In addition, we believe structural changes are necessary for CRCL to serve as an effective check on the Department’s operational units. For example, CRCL should be more transparent with people who file complaints with the office and ensure that it can make meaningful, independent reports to Congress and the public on its activities as well as DHS’s responses to its recommendations. It does not appear that CRCL has a role in reviewing the intelligence work of the Department’s operational components—but it should. To that end, one concrete change would be to revive CRCL’s regular reviews of the products of the Office of Intelligence and Analysis.<sup>21</sup>

\*\*\*

We look forward to working with your Department in implementing these recommendations and providing our expert knowledge on these critical issues.

American Civil Liberties Union  
American-Arab Anti-Discrimination  
Committee (ADC)  
Arab American Institute  
Asian Americans Advancing Justice – AAJC  
Bend the Arc: Jewish Action

Brennan Center for Justice  
Center for Constitutional Rights  
Center for Democracy & Technology  
Center for Digital Democracy  
Center on Privacy & Technology at  
Georgetown Law

---

<sup>20</sup> *Id.*; Rachael Levy, *Homeland Security Considers Outside Firms to Analyze Social Media After Jan. 6 Failure*, Wall Street Journal (Aug. 15, 2021), <https://www.wsj.com/articles/homeland-security-considers-outside-firms-to-analyze-social-media-after-jan-6-failure-11629025200> (“The effort, which remains under discussion and hasn’t received approval or funding, would involve sifting through large flows of internet traffic to help identify online narratives that might provide leads on developing attacks, whether from home or abroad.”); *Summary of Terrorism Threat to the U.S. Homeland*, Dep’t of Homeland Sec. (Aug. 13, 2021), <https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-august-13-2021> (“DHS will continue to identify and evaluate calls for violence, including online activity associated with the spread of disinformation, conspiracy theories, and false narratives, by known or suspected threat actors and provide updated information, as necessary.”).

<sup>21</sup> See Tia Sewell & Benjamin Wittes, *The Evolution of DHS Intelligence Review Policy*, Lawfare (Aug. 14, 2020), <https://www.lawfareblog.com/evolution-dhs-intelligence-review-policy>.

Citizens for Responsibility and Ethics in  
Washington  
Color of Change  
Demand Progress  
Electronic Frontier Foundation  
Electronic Privacy Information Center (EPIC)  
The Leadership Conference on Civil and  
Human Rights

Muslim Advocates  
National Council of Jewish Women  
Open The Government  
Project On Government Oversight  
Restore The Fourth  
The Sikh Coalition