May 31, 2022

Lynn Parker Dupree
Chief Privacy Officer / Chief FOIA Officer
U.S. Department of Homeland Security

Amanda Baran
Chief, Office of Policy and Strategy
U.S. Citizenship and Immigration Services

Dear Lynn Parker Dupree and Amanda Baran:

On behalf of members of the Immigrant Surveillance Working Group (ISWG) and the Denaturalization Strategy Group we would like to thank both of you, and your teams, for meeting with us in February. We appreciate your time and your interest in hearing our concerns related to the Department's denaturalization practices and use of technology.

At our meeting in February, you asked us to provide policy alternatives that could resolve the concerns around discriminatory profiling and overbreadth of surveillance. We have spent quite some time considering this request, which presents two challenges for us. First, many of our organizations, as advocates for liberty and freedom from discrimination, are challenged by providing the Department with alternatives that will continue to target immigrant communities of color. Second, we are unable to provide meaningful solutions without transparency from the Department on how programs like ATLAS operate and how the information collected is used.

The technologies at issue have dramatically shifted the Department's use of denaturalization by altering the ways in which individuals are targeted for denaturalization. Previously, denaturalization was used in rare and egregious occurrences such as for individuals who committed crimes against humanity. These individuals were typically brought to the attention of the Department rather than the Department seeking them out. Today, individuals are identified through extensive, sweeping, and onerous searches of their data, the specifics of which are shrouded in secrecy. Some of these searches are being initiated by the submission of an immigration benefit application through tools like ATLAS.[1] This has led to many more instances of denaturalization enforcement, beyond the rare and egregious instances of the past.

While we recognize that the Department under the Biden Administration has taken steps to deescalate denaturalization efforts, there is still substantial risk in continued reliance on these technologies and the lack of transparency surrounding their use. In an administration that strives to provide a sharp contrast to the previous administration we are gravely concerned, especially as we have so recently experienced how an administration hostile toward immigrant communities of color can further weaponize technology and tools such as denaturalization to target these communities.

[1] US Department of Homeland Security (DHS), "Privacy Impact Assessment for the ATLAS," DHS/USCIS/PIA-084, Oct. 30, 2020, available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis084-atlas-july2021.pdf [hereinafter ATLAS PIA]. *See* Community Justice Exchange, *From Data Criminalization to Prison Abolition*, 2022, available at: https://abolishdatacrim.org/en/report/full [hereinafter *From Data Criminalization*] ("An Application-Based Dragnet").

The Department's own governing policy on privacy and compliance[2] highlights the need for limitation and transparency when collecting the private information of individuals. A recent report from the Georgetown Law Center on Privacy and Technology[3] calls into question the Department's commitment to these tenets. While we remain grateful for the opportunity to engage with the Department and with your offices specifically through meetings and correspondence where you listen to our concerns, without an actual dialogue, our concerns remain elevated.

Below we present information on recent denaturalization cases so you can better understand the scope of how this tool impacts individuals and communities; a summary of our concerns; and a list of our recommendations. We hope you find this helpful and that the next step can involve sharing of information by the Department to shed light on our concerns.

I. Examples of Recent Denaturalization Cases

We start with a discussion of recent denaturalization cases involving individuals who were targeted by the Trump Administration to emphasize that denaturalization continues to harm individuals and communities under this administration. These cases highlight the critical role of technology and overly broad surveillance in enabling the government to target U.S. citizens who are deeply rooted in their communities after decades of living in the United States. For these cases, it is likely that the first step in identifying these individuals as targets for denaturalization was a flag, or System Generated Notification (SGN), created by ATLAS.[4] Moreover the grounds for denaturalization that the government alleges for the cases below make clear that denaturalization has drastically expanded from its practice in the last half century. Denaturalization has morphed into yet another immigration enforcement tool, intentional in its design[5], that seeks to punish, then deport, individuals that have already been subjected to the criminal legal system.

Luis Alberto Martinez came to the United States as a teenager from Mexico in 1997. He became a U.S. citizen in 2011, and he remembers the day he recited the naturalization oath as one of the proudest days of his life. Two years after he naturalized, Mr. Martinez was indicted for and pled guilty to one count of Medicaid Fraud, a third-degree felony in Texas. The trial court in his criminal case deferred adjudication of his guilt and sentenced him to two years of community supervision and a $750 fine. In 2019, over six years after Mr. Martinez's criminal case concluded and eight years after he naturalized, the United States instituted civil denaturalization proceedings against Mr. Martinez, alleging that he concealed his criminal activity arising from the Medicaid Fraud charge during the naturalization process. Despite Mr. Martinez's substantial ties to the United States, including two U.S. citizen children and decades long residence in the country, the Trump Administration targeted Mr. Martinez for revocation of his U.S. citizenship and the current administration continues to prosecute his denaturalization case (Case No. 7:19-cv-00345, S.D. Tex.). While it is unclear how the Department became aware of Mr. Martinez's case for potential denaturalization, it is highly likely that overbroad surveillance

[2] DHS, "Privacy Policy and Compliance Directive 047-01," July 7, 2011, available at: https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01.

[3] Georgetown Law Center on Privacy and Technology, *American Dragnet*, *Data-Driven Deportation in the 21st Century*, May 10, 2022, available at: https://americandragnet.org/ [hereinafter *American Dragnet*].

[4] *See* Sam Biddle and Maryam Saleh, *Little-Known Federal Software Can Trigger Revocation of Citizenship*, The Intercept (Aug. 25, 2021), available at: https://theintercept.com/2021/08/25/atlas-citizenship-denaturalization-homeland-security/ (reporting on a 2019 FOIA production by USCIS that included a flowchart showing an ATLAS System Generated Notification (SGN) as the first step in denaturalization investigations).

[5] *See* US Department of Justice, 65 U.S. Attorneys' Bulletin, July (I) 2017, at 1, available at: https://www.justice.gov/usao/page/file/984701/download (In a 2017 bulletin to federal prosecutors, then Attorney General Jeff Sessions describes civil denaturalization as "facilitat[ing] the Department of Homeland Security's ability to institute removal proceedings so that [denaturalized individuals] can be expeditiously removed from the United States").

technology was utilized as his case comes nowhere close to the rare circumstances in which denaturalization has been used historically.

Abderrahmane Farhane[6] moved to the United States in the 1990s from Morocco with his family, through the diversity visa lottery. After moving to Brooklyn, Mr. Farhane opened a few businesses, including a bookstore. He became a United States citizen in 2002, applying very shortly after becoming eligible. Four years after he naturalized, Mr. Farhane was charged with and pled guilty to one count of conspiracy to commit money laundering and one count of providing false statements to federal law enforcement investigators. Mr. Farhane had originally also been charged with conspiracy to provide material support to terrorists. Mr. Farhane was sentenced to 13 years and was released in 2017 for good behavior. A year later, in 2018, the United States instituted denaturalization proceedings against Mr. Farhane, alleging that he concealed his involvement in criminal activity arising from the conspiracy to commit money laundering charge during the naturalization process. Mr. Farhane has six children, all of whom are U.S. citizens, as is his wife. The Trump Administration targeted Mr. Farhane for revocation of his U.S. citizenship, despite his longstanding presence in the United States. By doing so, the government is not only targeting Mr. Farhane, but seeking Mr. Farhane's denaturalization also threatens the citizenship of Mr. Farhane's two U.S. citizen children who derived citizenship through him. Mr. Farhane's denaturalization case remains stayed (Case No. 1:18-cv-04347, E.D.N.Y.) while he seeks vacatur of his conviction and plea as the product of ineffective assistance of counsel, which is currently pending before the court of appeals (20-1666, 2d Cir).

II. Summary of Concerns Relating to DHS's Use of Technology in Denaturalization Enforcement and Beyond

In the February meeting, we outlined three areas of concern related to DHS's use of digital technology for surveillance-based anti-fraud, threat-detection and law enforcement techniques:

> (i) the **quality and accuracy of the data** used to execute the current "threat-based" approach to advancing DHS's broad mission;[7]
>
> (ii) the **content, operation and opacity of algorithms** used to process that data; and
>
> (iii) **limitations and shortcomings of mitigations** asserted or adopted to address the risks associated with use of bulk data and threat-based approaches to achieving the agency's goals.

For each area of concern, we presented both general and denaturalization-specific information to illustrate how these concerns arise and play out in practice.

Reliance on inaccurate data for immigration surveillance

The ubiquity of digital data is foundational to the agency's overreliance on dragnet-style methods for executing its mission.[8] As advocates, we are calling for a reconsideration and

[6] *See* Hannah Allam and Razzan Nakhlawi, *He pleaded guilty in a terrorism case and did his time. Now the government wants to strip him of his American citizenship*, The Washington Post (Dec. 18, 2021), available at: *https://www.washingtonpost.com/national-security/trump-biden-denaturalization-deportation/2021/12/18/e31c958e-5854-11ec-a219-9b4ae96da3b7_story.html* (covering Mr. Farhane and his case).

[7] *See* Center for American Progress, *Redefining Homeland Security: A New Framework for DHS to Meet Today's Challenges*, June 21, 2021, at 6, available at: https://www.americanprogress.org/article/redefining-homeland-security-new-framework-dhs-meet-todays-challenges/.

[8] *American Dragnet*, *supra* note 3 (noting the multiple and evolving pipelines for access to data, not only from government databases, but also from private data controllers and data brokers).

reversal of this data-driven approach.[9] As part of that call, we emphasize that in order to amass the partnerships and access that bring so much data within the processing power of DHS, the agency has prioritized quantity over quality.[10] Datasets that DHS's automated anti-fraud measures, enforcement and threat-detection operations draw on are known to contain inaccuracies, producing unreliable outcomes that can lead to devastating mistakes in benefits processing, detention, deportation, and denaturalization practices.[11]

ATLAS is an automated background check and screening tool used by USCIS in processing benefits applications and denaturalization.[12] A FOIA production by USCIS last year included a flowchart showing an ATLAS system generated notification (SGN) as the first step in denaturalization investigations.[13] The standard background checks run through ATLAS pull from a range of datasets, including IDENT, ABIS, FBI Name Check and TECS Name Check.[14]

In this context, we highlighted data accuracy and consistency concerns linked to two specific datasets identified as ATLAS sources. The concerns arising from inaccurate or unverified data and its use in disproportionately criminalizing and targeting Black and brown communities are in no way limited to just these two datasets.[15]

First, IDENT is a repository of biometric and biographical information that sits within a web of interconnected agency databases.[16] The Office of Biometric Identity Management (OBIM), the developer of the system within DHS, **only "recommends" that its many data suppliers maintain accuracy**.[17] As OBIM is not configured as the data owner, OBIM itself bears no responsibility for data accuracy.[18] IDENT is currently being replaced by HART, with a lifecycle cost to date of USD 6.158 billion according to a March 2022 Government Accountability Office (GAO) report.[19] HART introduces new and even more experimental biometrics matching modalities, including facial recognition,[20] and increased processing capacity, **eliminating a practical constraint on expanding the use of programs like ATLAS** without any

[9] *See, e.g.*, Immigrant Legal Resource Center with 96 signatories, *Denaturalization Priorities*, Oct. 27, 2021, available at: https://www.ilrc.org/denaturalization-priorities#:~:text=The%20ILRC%2C%20along%20with%2096,belongs%20in%20the%20United%20States [hereinafter *Denaturalization Priorities*]; Immigration Surveillance Working Group, *Coalition Partners Letter to Secretary Mayorkas*, Sept. 15, 2021, available at: https://www.brennancenter.org/our-work/research-reports/coalition-partners-send-letter-homeland-security-secretary-alejandro [hereinafter *Coalition Partners Letter*]. *See also American Dragnet*, *supra* note 3; Community Justice Exchange, *From Data Criminalization*, *supra* note 1; Immigrant Defense Project, Just Futures Law & Mijente, *HART Attack: How DHS's massive biometrics database will supercharge surveillance and threaten rights*, May 2022, at 32, available at: https://justfutureslaw.org/wp-content/uploads/2022/05/HART-Attack.pdf [hereinafter *HART Attack*].

[10] *American Dragnet*, *supra* note 3.

[11] *See, e.g.*, *Gonzalez v. United States Immigr. & Customs Enf't*, 416 F. Supp. 3d 995 (C.D. Cal. 2019), *rev'd on other grounds*, 975 F.3d 788 (9th Cir. 2020).

[12] ATLAS PIA, *supra* note 1.

[13] *See* Biddle and Saleh, *supra* note 4.

[14] DHS Privacy Office, "2019 Data Mining Report to Congress," Dec. 2, 2020, available at: https://www.dhs.gov/sites/default/files/publications/2019_data_mining_report_final_12-2-20.pdf [hereinafter 2019 Data Mining Report].

[15] *See* ATLAS PIA, *supra* note 1 at 30 (listing ATLAS Connections and Data Sources for Screening); *see also, e.g.*, *Coalition Partners Letter*, *supra* note 9 (discussing concerns relating to the Automated Targeting System (ATS)); *From Data Criminalization*, *supra* note 1.

[16] *Gonzalez*, 416 F. Supp. 3d 995 (Findings of Fact and Conclusions of Law).

[17] US Department of Homeland Security, "Homeland Advanced Recognition Technology System (HART) Increment 1 Privacy Impact Statement (PIA)," DHS/OBIM/PIA-004," February 24, 2020, available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf [hereinafter HART Increment 1 PIA].

[18] HART Increment 1 PIA, *supra* note 17; *HART Attack*, *supra* note 9 at 32.

[19] US Government Accounting Office (GAO), "DHS Annual Assessment: Most Acquisition Programs Are Meeting Goals Even with Some Management Issues and COVID-19 Delays," GAO-22-104684, March 8, 2022, at 39, available at: https://www.gao.gov/assets/gao-22-104684.pdf. *See HART Attack*, *supra* note 9.

[20] GAO, "Facial Recognition Technology: Current and Planned Uses by Federal Agencies," GAO-21-526, Aug. 2021, at 56, available at: https://www.gao.gov/assets/gao-21-526.pdf [hereinafter GAO Report on Facial Recognition Technology].

corresponding assurances that DHS is examining the necessity, sourcing approach, ownership and control, structure and accuracy of the data it will use for these processes.[21]

Second, ATLAS also links to Nlets through TECS Name Check.[22] Nlets is a massive clearinghouse of state and local law enforcement and commercial data gathered since the 1990s, hosted by a non-governmental entity, which processes an estimated 1.6 billion transactions annually.[23] Nlets is also connected to COPLINK and CLEAR, two data sources **criticized for unregulated sharing of unverified information including race, ethnicity and national origin data**.[24] Local data entry and processing practices vary widely across the entities feeding information into Nlets, and the **aggregation of that data in a tools like COPLINK has the effect of flattening out these inconsistencies**, so that all tags for "gang affiliation," for instance, may be granted equal weight without any review for bias and disparate impact.[25]

With respect to denaturalization, we specifically raised data accuracy and reliability concerns related to (i) nationality, citizenship, and legal status determination; and (ii) the use of digitized fingerprint data for identification.

First, the agency's own **inconsistent recording and lack of rigor in maintaining records on nationality and country of origin information** is a pervasive issue that was identified by former personnel responsible for denaturalization cases and training interviewed for the report *Unmaking Americans: Insecure Citizenship in the United States*.[26] This is a concern, for example, because country of origin information data are known to be used in identifying potential fraud patterns.[27] As a result of this practice, nearly half of all denaturalization cases filed in 2017 and 2018 targeted U.S. citizens whose country of origin data matched them with known "special interest" countries.[28]

Second, since Operation Janus,[29] denaturalization cases often hinge on one piece of evidence, a digital fingerprint match, to support the government's claim that the defendant acquired citizenship illegally.[30] Even in highly controlled, laboratory circumstances, **digital fingerprint matching is far from error-free**.[31] Since 2011, DHS has been digitizing approximately 2 million

[21] *See HART Attack*, *supra* note 9, at 29-37.

[22] DHS, "Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing," Dec. 22, 2010, available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf; National Immigration Law Center, "Nlets: Questions & Answers," Nov. 2020, available at: https://www.nilc.org/wp-content/uploads/2020/11/Nlets-Q-and-A.pdf.

[23] *American Dragnet*, *supra* note 3.

[24] Joseph, George, *New Documents Reveal How ICE Mines Local Police Databases Across The Country*, The Appeal (Apr. 26, 2018), available at: https://theappeal.org/new-documents-reveal-how-ice-mines-local-police-databases-across-the-country-660e2dfddbe3/.

[25] *Id.*; DHS, "Privacy Impact Assessment for Fraud Detection and National Security Data System (FDNS-DS)," DHS/USCIS/PIA-013(a), May 18, 2016, at 5, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-fdnsds-november2017.pdf (ATLAS mines data to identify "non-obvious relationship" patterns); 2019 Data Mining Report, *supra* note 14.

[26] Open Society Justice Initiative, *Unmaking Americans: Insecure Citizenship in the United States*, 2019, available at: https://www.justiceinitiative.org/publications/unmaking-americans [hereinafter *Unmaking Americans*]. *See also Gonzalez*, 416 F. Supp. 3d 995 at 1004 ("An individual's citizenship and immigration status is not static and may change multiple times over a lifetime. [internal citations omitted]").

[27] *See, e.g.*, *Unmaking Americans*, *supra* note 26.

[28] *Unmaking Americans*, *supra* note 26 at 2, 96.

[29] DHS Office of Inspector General (OIG), "Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records," OIG-16-130, Sept. 8, 2016, available at: https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/2016/OIG-16-130-Sep16.pdf [hereinafter 2016 DHS OIG report].

[30] *Unmaking Americans*, *supra* note 26.

[31] *See, e.g.*, NYU Center for Human Rights and Global Justice and Temple Institute for Law, Innovation & Technology (iLIT), Response to Request for Information (RFI) FR Doc. 2012-21975, to the White House Office of Science and Technology Policy (OSTP) (January 2022), notes 27-36 and accompanying text, available at: https://chrgj.org/wp-content/uploads/2022/01/CHRGJ_iLIT_OSTP_RFI_Biometrics_Response-January-2022.pdf.

physical fingerprint files originally taken using ink and card stock in the 1990s and 2000s.[32] The age and quality of these source records gives us concerns about the accuracy and reliability, particularly as no public information exists on the thresholds used for identifying a true match and the risks of false positives. The context in which the original fingerprint impressions were taken also gives reason to doubt the accuracy of the biographical information attached to the biometric information captured on a card file.[33]

In 2019, the *New York Times Magazine* extensively covered a Florida denaturalization case in which the trial court **refused to consider evidence challenging the accuracy and reliability of newly digitized historical fingerprint evidence**.[34]

Reliance on unaccountable algorithms and evidence of algorithmic bias and discriminatory outcomes

We refer you to previous, more comprehensive treatment of DHS's use of automated data processing, a critical area of concern covered in a report by Community Justice Exchange.[35] With respect to the ATLAS software specifically, the 2020 Privacy Impact Assessment expressly reserves the agency's discretion to use race or ethnicity data for ATLAS operations, including to attribute a connection to a particular country, as a "screening criterion."[36] The use of race or ethnicity data to draw conclusions about (legal) nationality, even for screening purposes, implies that the agency is using racialized assumptions about citizenship and legal status as part of the process of automating its operations.

In denaturalization cases, as noted above, DHS and DOJ have been clear about the use of country of origin information as part of the screening and targeting process used to carry out wide-scale denaturalization operations like Janus and Second Look.[37] ATLAS SGNs trigger denaturalization investigations.[38] We therefore have **serious concerns regarding the automated use of race and ethnicity data as the basis for expanding denaturalization** prosecutions far beyond their decades-long purpose as an accountability tool for war criminals living in impunity in the U.S. We are also concerned that the source of race and ethnicity data on any individual is currently untraceable.

Relatedly, the **ATLAS software plays a central role in drastically scaling up the use of denaturalization** from a tool reserved for war criminals to a generalized enforcement measure,

[32] *See Unmaking Americans*, *supra* note 26. In response to FOIA requests, USCIS produced materials stating that at least 2 million records were to be digitized, which is much greater than the original figure mentioned in the 2016 DHS OIG report (315,000). *See, e.g.*, Open Society Justice Initiative, *Document Cloud, USCIS Documents 1: January 2021*, at 204, available at: https://www.documentcloud.org/documents/21049099-uscis-documents-1-january-2021.

[33] *Unmaking Americans, supra* note 26 at 101 ("In 1994, an inspector general's report as well as a DOJ study found that INS (a predecessor agency to DHS) could not verify that fingerprints on cards belonged to the applicants listed on the top portion of the card.").

[34] Wessler, Seth Freed, *Is Denaturalization the Next Front in the Trump Administration's War on Immigration?*, N.Y. Times Magazine (Dec. 19, 2018), available at: https://www.nytimes.com/2018/12/19/magazine/naturalized-citizenship-immigrationtrump.html (covering Ms. Odette Dureland's case). *See Unmaking Americans*, *supra* note 26 at 93-94 ("In [multiple identities] cases, the government proceeds with referring to the defendant by the name the government determines is the defendant's *real* name, not necessarily the name the defendant asserts as their true name. The entire proceeding signals the guilt of the defendant in using a "false" name as a foregone conclusion in such cases.").

[35] *From Data Criminalization*, *supra* note 1. *See also* 2019 Data Mining Report, *supra* note 14.

[36] ATLAS PIA, *supra* note 1 at 8 (stating that it "prohibit[s] the consideration of race or ethnicity in investigation, screening, and law enforcement activities in all but the most exceptional instances and limit[s] the consideration of an individual's simple connection to a particular country, by birth or citizenship, as a screening criterion, unless such consideration is based on an assessment of intelligence and risk and in which alternatives do not meet security needs.")

[37] *See* 2016 DHS OIG report, *supra* note 29 at 1 n.1.

[38] *See* Biddle and Saleh, *supra* note 4.

which advocates have consistently cited with alarm and this administration set out to address through President Biden's Executive Order on Restoring Faith in Our Legal Immigration Systems and Strengthening Integration and Inclusion Efforts for New Americans.[39]

The **lack of algorithmic transparency** has likewise been comprehensively addressed by advocates, both directly in previous meetings and written communication with DHS, and through independent research and reporting.[40] The ATLAS algorithm's rules are not public or made available for independent review.[41] No disaggregated data is available to independent researchers or to the public on the outcomes of automatically-generated flags (like ATLAS SGNs). We do not know, for instance, what percentage of flags result in enforcement actions, or what percentage are actually false positives, and how the agency responds to this information.[42] As noted above, significantly more transparency is needed regarding the role that race and ethnicity play in triggering denaturalization investigations and prosecutions. Given the concerns noted above with respect to the centrality and potential unreliability of fingerprint matching processes in denaturalization cases, independent auditing including disparate impact assessments are needed for the algorithms used to perform these operations.

Insufficiency of mitigation measures

The choice to privilege digital surveillance across so many of DHS's functions perpetuates an operating environment that is **heavily prejudiced in favor of promoting and defending data-driven outcomes**.[43] This operating environment has important implications for risk tolerance within DHS, including the internal evaluation of risk mitigation. In the February meeting, advocates highlighted several examples to illustrate how DHS's current practices for risk assessment and mitigation fail to address the well-documented concerns we have outlined.

For instance, the ATLAS PIA states that DHS **assumes that information contained in source databases is accurate**.[44] Based on the above summary of data accuracy and reliability concerns, drawing on extensive research and documentation by advocates, such an assertion is both irrational and negligent. In fact, we know that reliance on inaccurate data has resulted in grave mistakes, such as the false imprisonment of hundreds of U.S. citizens,[45] and yet **no publicly available risk assessments suggest that DHS investigates the individual and community impact of false positives** through processes employing biometric identification (like Operation Janus-style historical fingerprint evidence matching) or algorithmic screening (like ATLAS).[46] The Fraud Detection and National Security Data System PIA notes that USCIS"continually tunes the rules to narrow the scope of information [processed] . . . and reduce potential for false positives," without discussing how the agency measures and weighs

[39] Executive Order on Restoring Faith in Our Legal Immigration Systems and Strengthening Integration and Inclusion Efforts for New Americans, E.O. 14012 (Feb. 2, 2021), available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/02/executive-order-restoring-faith-in-our-legal-immigration-systems-and-strengthening-integration-and-inclusion-efforts-for-new-americans.

[40] *Denaturalization Priorities*, *supra* note 9; *Coalition Partners Letter*, *supra* note 9.

[41] *See* Open Society Justice Initiative, Freedom of Information Act (FOIA) Request on ATLAS, Aug. 25, 2021, available at: https://www.justiceinitiative.org/uploads/bbfbcc55-9158-4a6c-a259-2ee4c5ef3d90/denatz-osji-foia-request-atlas-08252021.pdf.

[42] 2019 Data Mining Report, *supra* note 14, at 54-55 ("Efficacy").

[43] *American Dragnet*, *supra* note 3.

[44] ATLAS PIA, *supra* note 1.

[45] *Gonzalez*, 416 F. Supp. 3d 995 at 1011 (discussing evidence of U.S. citizens wrongly subject to detainers because of database errors).

[46] *See, e.g.*, ATLAS PIA, *supra* note 1; DHS, "Privacy Impact Assessment for the Fraud Detection and National Security Data System (FDNS-DS)," DHS/USCIS/PIA-013(a), May 18, 2016, available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-fdnsds-november2017.pdf [hereinafter FDNS-DS PIA].

the costs of previously overinclusive rules and/or data inaccuracies that caused the overbreadth of its previous practice.[47]

Given widespread criticisms and heightened scrutiny[48] of the risks of facial recognition technology (FRT), DHS's risk assessment practice is especially out of step, even as DHS is expanding use of this technology under this administration.[49] In the September 15, 2021 Immigrant Surveillance Working Group coalition letter, advocates raised concerns about Custom and Border Protection's (CBP) Automated Targeting System (ATS). In the most recent (2017) PIA update for ATS, the only mitigation listed for FRT "imprecision" is FBI training to CBP officers to "assist with match determination."[50]

Based on years of research by advocates, the public is increasingly aware of the unprecedented scope of DHS's data processing power, both its breadth and its intrusiveness into public and private life.[51] Yet DHS's internal assessments do not meaningfully engage with the systemic risks attached to this reality. The HART PIA, for example, acknowledges an unmitigated risk that individuals will not know how their biometrics are stored, shared and used, without further discussion.[52]

In denaturalization cases, the available risk assessments for specific technologies and components of DHS **do not reflect adequate consideration of the potential individual and social impacts of the process (denaturalization investigation and prosecution) and ultimate outcome (citizenship-stripping) for which these technologies are used**.

Approximately one in four denaturalization cases in 2017 and 2018 ended in settlements that included judicial removal orders or terms waiving defenses to removal and other forms of protection.[53] One in four civil defendants had no representation.[54] Defendants can be removed while they appeal their case.[55] Each of these **due process concerns within the denaturalization process heightens the risk that data inaccuracies and algorithmic bias will remain unaccounted for and unchallenged**.[56]

DHS's self-assessment of the ATLAS software also **does not differentiate between different use cases, suggesting that the same mitigations are viewed as sufficient for all potential use cases**, whether the end result of an SGN is a denial of a benefit or a retroactive civil denaturalization decades after the individual concerned became a U.S. citizen, as in the case of Luis Alberto Martinez.

[47] FDNS-DS PIA, *supra* note 46 at 20.

[48] European Commission (2021), *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts,* COM/2021/206 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC02062. The draft European Union AI Act includes strict limitations on the use of facial recognition technology with many influential policymakers and advocates calling for a ban on the use of the technology altogether. *See* Melissa Heikkilä, "A quick guide to the most important AI law you've never heard of," MIT Technology Review, May 13, 2022, available at https://www.technologyreview.com/2022/05/13/1052223/guide-ai-act-europe/; Ada Lovelace Institute, *The EU AI Act: a summary of its significance and scope*, April 2022, available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf.

[49] GAO Report on Facial Recognition Technology, *supra* note 20.

[50] DHS, "Privacy Impact Assessment Update for the Automated Targeting System," DHS/CBP/PIA-006(e), Jan. 13, 2017, at 18, available at: https://www.dhs.gov/sites/default/files/2022-05/privacy-pia-cbp006%28e%29-ats-may2022.pdf.

[51] *American Dragnet*, *supra* note 3.

[52] HART Increment 1 PIA, *supra* note 17.

[53] *Unmaking Americans, supra* note 26.

[54] *Id.*

[55] *Id.*

[56] *See* Allam and Razzan, *supra* note 6 (covering Mr. Farhane's case).

The concerns raised by our coalitions over the course of this administration have been met with words of reassurance and actions that tell another story. We concluded the February meeting by emphasizing that now is the time to act to scale back the surveillance powers of this agency and reorient its operational mentality away from overreliance on data, perpetual vetting,[57] and collective suspicion.

III. Recommendations[58]

The following recommendations address the intersection of denaturalization and technologies, which was the focus of our joint meeting with DHS Privacy and USCIS. While any meaningful change to denaturalization policy must address the technologies underlying the denaturalization apparatus, these recommendations alone are inadequate to address the expanded use of denaturalization as yet another immigration enforcement tool. In our previous letter dated October 27, 2021, we, along with 96 signatories, provided recommendations on actions that this Department can take to address concerns arising from the current use of denaturalization at large.[59]

First and foremost, we ask for transparency. Transparency is a prerequisite to a "culture of privacy" within the Department. It is also a starting point to addressing the concerns presented, and a path to better engagement with civil society and impacted communities on solutions. During our joint meeting, the Department requested recommendations to address the issues we raised and while we are able to provide the following recommendations, transparency is key to meaningful engagement. To this end, we ask the Department to:

- Provide public disclosure of the rules that ATLAS is using to flag individuals for further investigation; the population being flagged by ATLAS, disaggregated by race, country of origin, etc.; the number of screenings and flags/System Generated Notifications (SGNs), and the outcome of those flags, including data on how many SGNs end up in denaturalization investigation and prosecutions and other enforcement actions.
- Provide a roadmap of how ATLAS is being used by mapping out the kinds of information and databases that ATLAS screens through; the purposes for which it is used, e.g. denaturalization or other civil or criminal enforcement actions; and how it flows within the Department and to other agencies.

While transparency is a necessary first step, transparency alone will not address the concerns presented or the harms to targeted communities. We urge the Department to take the following next steps:

[57] *See Coalition Partners Letter*, *supra* note 9 (discussing Continuous Immigration Vetting (CIV); 2019 Data Mining Report, *supra* note 14.

[58] These recommendations were also included in previous letters addressed to Secretary Mayorkas by the Denaturalization Working Group and Immigrant Surveillance Working Group. *Denaturalization Priorities*, *supra* note 9 (sent by Immigrant Legal Resource Center, along with 96 signatories), available at: https://www.ilrc.org/denaturalization-priorities#:~:text=The%20ILRC%2C%20along%20with%2096.belongs%20in%20the%20United%20States; *Coalition Partners Letter*, *supra* note 9 (sent by Immigration Surveillance Working Group coalition), available at: https://www.brennancenter.org/our-work/research-reports/coalition-partners-send-letter-homeland-security-secretary-alejandro.

[59] *Denaturalization Priorities*, *supra* note 9, available at: https://www.ilrc.org/denaturalization-priorities#:~:text=The%20ILRC%2C%20along%20with%2096.belongs%20in%20the%20United%20States.

- Halt the use of ATLAS and other technology used to flag individuals for further investigation pending a data protection and disparate impact review. Specifically:
    - Conduct and publish an independent disparate impact analysis of ATLAS, which would audit both the rules and data for bias in denaturalization cases.
    - Integrate an independent review of the role and impact of data-driven technologies to scale DHS's anti-fraud operations as part of the roadmap to reforming denaturalization within USCIS and partner components and agencies.
    - Work across agency sub-components to identify and effectively mitigate risks of biased, unreliable, and inaccurate data informing automated decisions.
    - Commit to a revised data governance framework within DHS and data-sharing partners that entails clear lines of agency accountability for the accuracy, necessity and veracity of all information collected and processed in connection with benefits adjudication and enforcement activities.
- Suspend the development of the Homeland Advanced Recognition Technology (HART) and divert funding for HART to ensuring access to immigration benefits instead.
- Suspend the purchase, acquisition, and processing of commercial and social media data within DHS systems, including the Automated Biometric Identification System (IDENT) currently in operation**.**
- Facilitate dialogue with immigrants' rights, racial justice and privacy/digital rights advocates to better coordinate resources as USCIS increases the automation of its processing activities.

Finally, we ask the Department to review recent denaturalization cases starting with cases initiated under Operation Janus and establish a process to make whole individuals who were denaturalized or impacted as derivatives, including through the reconsideration and restoration of legal status, so as to rectify the impacts of ATLAS and other technology on scaling discriminatory targeting. We also request that any denaturalization proceedings currently open be halted while a review of these processes is underway.

Signed,

Access Now
Asian Americans Advancing Justice | AAJC
Asian Americans Advancing Justice - Asian Law Caucus
Center on Privacy & Technology at Georgetown Law
Creating Law Enforcement Accountability & Responsibility Clinic at CUNY School of Law
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
Government Information Watch
Immigrant Defense Project
Immigrant Legal Resource Center
Institute for Law, Innovation & Technology at Temple Law
Just Futures Law
Muslim Advocates

National Immigrant Justice Center
National Immigration Project (NIPNLG)
Project on Government Oversight
Restore The Fourth
Surveillance Resistance Network
Surveillance Technology Oversight Project (S.T.O.P)