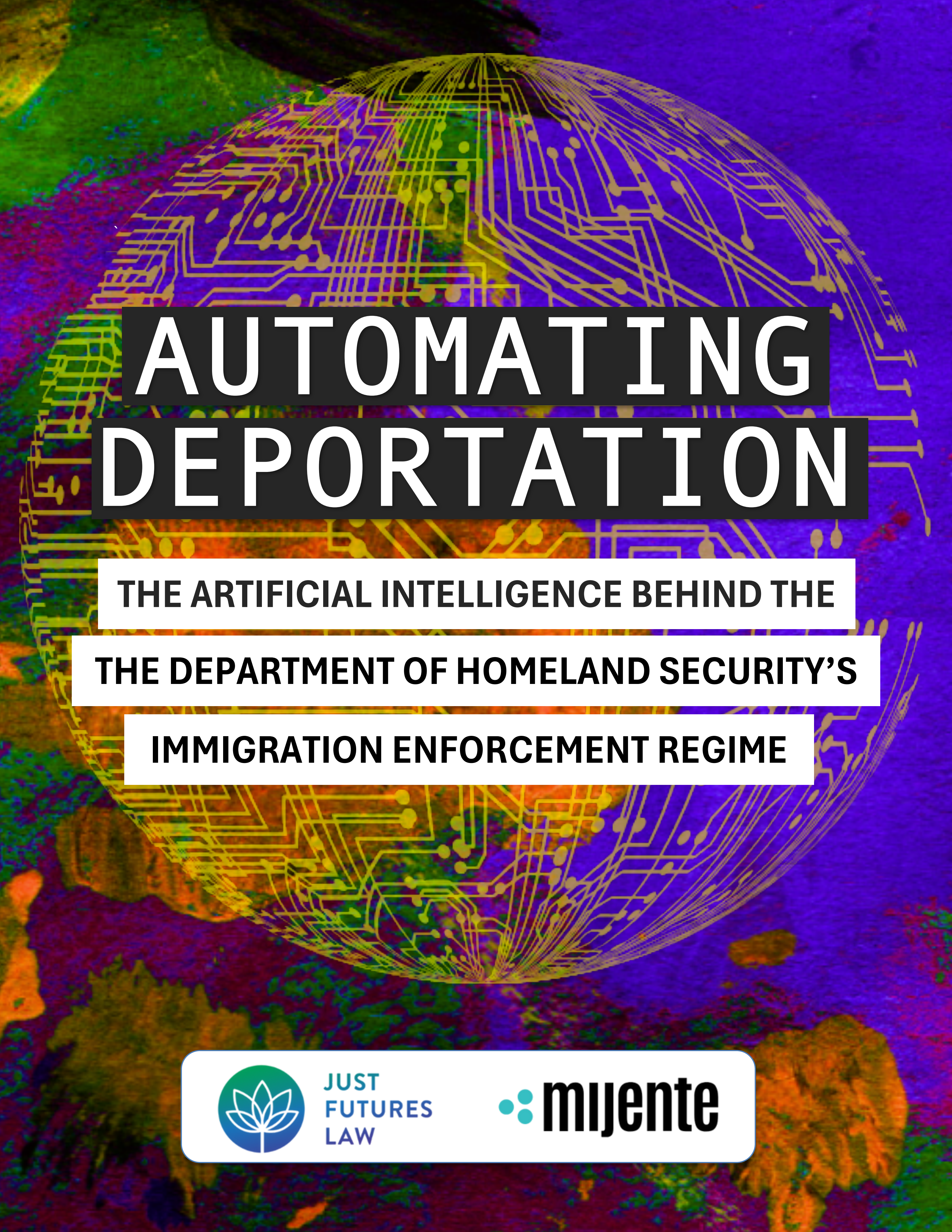


AUTOMATING DEPORTATION

THE ARTIFICIAL INTELLIGENCE BEHIND THE THE DEPARTMENT OF HOMELAND SECURITY'S IMMIGRATION ENFORCEMENT REGIME

JUST FUTURES LAW

mijente

ACKNOWLEDGEMENTS

Writers and Editors:

Julie Mao, Paromita Shah, Hannah Lucal,
Aly Panjwani, Jacinta Gonzalez

Researchers:

Aly Panjwani, Aaron Lackowski, Marina de la Sierra

Design:

Mayra Hernandez, Mijente

Special thanks to Empower LLC,
Jesse Franzblau, and Akina Younge

Published June 2024

Table of Contents

I. Introduction

Corporations are peddling "artificial intelligence" (AI) as the cure-all tool that can solve big social problems and improve our daily lives. Despite a lack of laws regulating AI, our federal and local governments are embracing AI without reservation – procuring tools, programs and systems without understanding how AI impacts communities or questioning whether they should deploy AI in the first place.

From healthcare to social services to military weapons to migration, AI threatens to automate answers to our society's most important questions, leaving the decision making to a secret machine that people know little about, let alone have the power to control. The Department of Homeland Security (DHS) has been using AI-like technologies for over a decade. But the hype around generative AI, such as the high profile release of ChatGPT, has launched a government funding frenzy. This year, Congress appropriated $3 billion across federal agencies to purchase and use AI.[1] With global private AI investment expected to reach $200 billion, the financial incentives for companies and governments to fast-track AI are significant.[2] Corporations and governments are scrambling to deploy AI tools at a rapid pace, with little concern for the civil and human rights consequences. Unfortunately, the AI arms race is outpacing government regulation, posing serious threats to millions of immigrants, U.S. communities and beyond.

When it comes to the federal government, there is perhaps no other sector racing to adopt AI more than U.S. migration and defense agencies. The Department of Homeland Security in conjunction with corporations has aggressively pushed the idea that AI will make immigration processing more efficient, more objective and less biased. Many of the same companies pushing AI hype have won lucrative AI contracts with DHS.[3] As our research shows, AI tools are now pervasive at DHS – agency decision makers use AI to make a range of decisions that impact people's lives, from adjudicating immigration benefits to designating people as "public safety threats" to locating individuals for detention and deportation. Just this year, DHS released an AI roadmap, detailing how AI will be used in its core missions.[4]

DHS has released policy language in support of civil rights and privacy and against systemic bias and discrimination.[5] However, as we explain in Section I.C. of this report, DHS is both side stepping its own policy requirements and failing to meet the federal government's minimum requirements for responsible deployment of AI. As such, DHS's fast-tracking of AI threatens to worsen the existing discriminatory practices of the immigration system without our knowledge, while also violating civil and privacy rights of millions of immigrants, families, and the larger U.S. community.

A. Research and Findings

This report surveys DHS use of artificial intelligence, pulling from years of research into AI tools at DHS and new information revealed by the DHS "AI Inventory." As discussed below, the Biden Administration's AI Executive Order, issued in October 2023, requires DHS to provide the public with information about its use of AI.

Our research found that DHS has prioritized the use of artificial intelligence at an aggressive pace across its sub-agencies, U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), despite the potential negative impacts and with almost no input from the public or affected communities. This report highlights a number of concerning uses of AI by DHS. While prior research focused on ICE and CBP use of technologies for detention and deportation efforts, these findings focus on a new and emerging use of AI to automate decision making, particularly at USCIS. Key findings include:

- **USCIS uses AI to help make automated decisions on immigration relief and benefits applications.** For example, USCIS created "Predicted to Naturalize," an AI tool that recommends decisions on U.S. citizenship applications (also known as naturalization applications). Additionally, USCIS created the "Asylum Text Analytics" program, an AI tool that automatically queries millions of asylum and withholding applications to determine which applications are deemed fraudulent. USCIS is also developing an AI tool to help the agency identify and deny immigration benefits to people that it labels fraud, public safety or national security threats.

- **ICE uses the "Hurricane Score" and the "Risk Classification Assessment" (RCA), seemingly AI-powered tools, that make decisions on whether to release a person from detention or determine the terms of their electronic surveillance** under ICE's Intensive Supervision Appearance Program (ISAP), the agency's electronic monitoring program for immigrants released from detention.

Additionally, in the Appendix of this report, we highlight three other alarming areas where DHS has deployed artificial intelligence: AI for processing data to conduct immigration enforcement, AI for powering the deadly digital border wall, and AI for biometric surveillance.

B. So What? A Call for AI Accountability at DHS

The implications of DHS using AI to automate its most critical, rights-impacting decisions is vast. AI may heavily influence or justify millions of DHS decisions – from whether to deport, detain, and separate families, to whether to naturalize someone, or protect someone from persecution or torture. The Department of Homeland Security (DHS) has, at some point or another, impacted 46 million foreign born persons in the United States.[6] USCIS processes 8 million applications annually, handling everything from work permits to temporary statuses to green cards to 875,000 naturalization applications.[7] The 2.8 million cases in the U.S. immigration courts, called the Executive Office for Immigration Courts (EOIR), often require USCIS findings to determine whether to order deportation or grant relief.[8] In short, family members, workers, students, DACA recipients, tourists, people fleeing persecution, and many more have their lives hanging on the decisions of USCIS, ICE and CBP.

U.S. Department of State
NONIMMIGRANT VISA APPLICATION
USCIS
Form N-600
Application For Naturalization
Form N-600, Application for Certificate of Citizenship
Part 1. Information About Your Eligibility
GUARDIAN R

DHS Obligations for Responsible AI

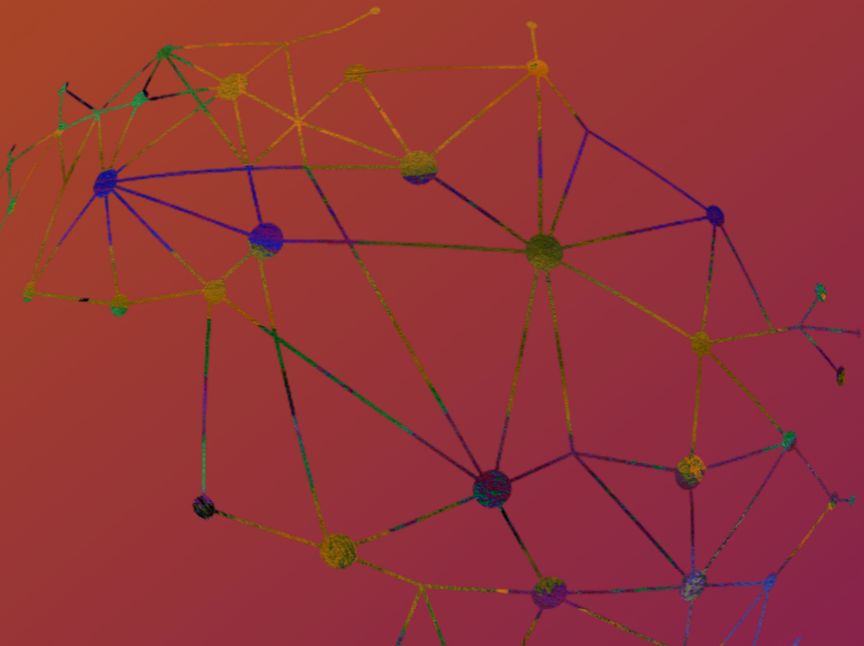
Recently passed law, executive orders, and agency memoranda require that DHS adopt key steps around responsible AI within the agency and *take the lead* in establishing standards across the federal government.[9] As early as December 2022, Congress required that DHS implement policies on AI use and civil rights in accordance with the Advancing American AI Act.[10] Subsequently, in August 2023, DHS released a memo on the use and acquisition of AI as required by this new law. It included strong language on protecting civil rights and limiting surveillance.[11] For example, the memo states:

> ***DHS will not use AI to improperly profile, target or to discriminate against any individual, or entity, based on the individual characteristics identified above, as reprisal or solely because of exercising their Constitutional rights. DHS will not use AI technology to enable improper systemic, indiscriminate, or large-scale monitoring, surveillance or tracking of individuals.***

Furthermore, on October 30, 2023, the Biden Administration issued Executive Order 14110, a directive for the governance of responsible AI in the federal government.[12] And in March 2024, the Office of Management and Budget (OMB), a federal agency that provides operations guidance to federal agencies, released a binding memorandum to all federal agencies, “Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence” (herein “OMB memo”). This OMB memo provided a detailed and lengthy risk assessment framework for “rights-impacting” and “safety-impacting” AI to protect access to critical services, protect equitable access to government services, reduce algorithmic bias, and protect civil rights from potential AI harms.[13]

Taken together, these memos, Executive Order, policies and laws on AI require DHS to:

- Designate a Chief Artificial Intelligence Officer (CAIO).[14] In the case of DHS, the CAIO is the Chief Information Officer Eric Hysen.
- Create a list of AI uses that are "presumed" to be "rights-impacting." This list covers any AI tool for immigration processing, enforcement and detention, and law enforcement technologies like facial recognition or GPS tracking.[15]
- Regularly monitor products for bias and discrimination or complete the required AI Impact Assessments (AIA) that will assess the technologies' expected benefits, risks, quality and appropriateness of the data, and the ways it can impact civil rights and privacy.[16]
- Publish AI products in a federal "inventory" on the agency website.[17]
- Notify affected individuals when the use of AI results in an "adverse decision or action that specifically concerns them," and create a process for "redress" if the AI decision was in error.[18]
- Consult with the public or impacted communities before the release of an AI product, and release the AI code, model, and training data to the extent possible.[19]
- Offer a mechanism to "conveniently" opt-out from the use of AI in favor of a human "alternative", such as, for example, a human adjudicator.[20]
- Require compliance with obligations by December 1, 2024 unless the agency can assert an exemption or obtain approval of a waiver or extension from the CAIO. If compliance is not reached or the CAIO does not approve the waiver or extension, then the agency must suspend or terminate use of a rights-impacting AI tool by December 1, 2024.[21]



Unfortunately, the new requirements allow several loopholes for national security, intelligence and law enforcement that may enable agencies to avoid compliance with these rules. Further weakening the integrity of these requirements, the CAIO has discretion to waive or exempt any part of the rights-impacting risk framework. For example, agencies can request that the CAIO waive an "opt-out" requirement if it causes "undue hardship on the agency."

C. Recommendations for DHS and the Biden Administration

We are highly concerned that there is little stopping immigration agencies from using AI to justify expanding detention and deportation targeting Black, Brown and immigrant communities. Despite the AI Executive Order and accompanying federal law and policies, our research shows that DHS has remained secretive about its use of AI and has not provided information to prove that its use of AI will not cause harm to immigrant communities. For example, even with its AI Inventory, DHS has provided little information about its AI programs – what data is going in, what results or recommendations are going out, how they work, or how DHS identifies or manages errors or conducts oversight.[i] In the meantime, DHS continues to purchase and use these powerful technologies on immigrant communities and beyond.

[i] Furthermore, we found that the DHS AI Inventory provides an incomplete list of AI tools that DHS uses or is developing. Moreover, from our months of reviewing DHS' AI website, we observed that DHS adds, deletes, and modifies AI programs with no explanation. When one JFL researcher reached out to the DHS CIO office to ask why some of the USCIS AI programs were removed from the website in November 2023, the office responded by putting the USCIS AI programs back on the website and gave no further explanation.

When it comes to civil rights protections for AI, DHS appears to be giving lip service without taking steps to comply with even the most basic requirements to reduce the impact of civil rights abuse and discrimination. As the lead agency charged with ensuring all federal government agencies use AI in a responsible way, DHS should suspend and cancel its use of any AI tool until it fixes its violations and proves it can comply with existing rules. If DHS fails to do so, the Biden Administration must step in to enforce its own policies and existing laws.

Recommendations:

1. **DHS and its sub-agencies should suspend and cancel the use or development of any artificial intelligence technologies used in immigration adjudication or immigration enforcement by December 1, 2024.** DHS has not complied with its obligations under the AI Executive Order, the OMB memo and other applicable laws and policies. Additionally, there is no evidence that DHS is complying with its own 2023 memorandum on using and purchasing AI.[22] If DHS does not fix these violations, the agency must suspend or terminate the AI tools discussed in this report by December 1, 2024. See figure 1 below for a summary of key violations.

2. **DHS Chief Information Officer (CIO) Eric Hysen should enforce the sunsetting of these "rights-impacting" AI tools by the required deadline of December 1, 2024 if the agency cannot meet compliance. The CIO should not waive or exempt any non-compliant AI tool.** As referenced above, the DHS CIO has discretion to approve exemptions, waivers and extensions at the request of the agency. For example, DHS AI programs can escape oversight if the CAIO exempts intelligence and law enforcement-related technologies as "critical agency operations." If the DHS CIO liberally approves waivers, the new AI obligations would be effectively meaningless, allowing agencies to avoid scrutiny and deploy harmful technologies that do not meet minimum safeguards.

3. **The Biden Administration must order DHS to cease use of AI in “rights-impacting” cases if DHS continues to blatantly violate or waive its AI requirements after December 1, 2024.** The Biden Administration must step in and order DHS to cease the use of these harmful AI tools if blatant failures of accountability persist at the agency. Otherwise, DHS would be left to self-enforce the AI requirements and rubber stamp its noncompliant AI tools.[28] Moreover, it should go without saying that DHS should not be using tools that produce discriminatory outcomes. Inaction would be glaring evidence that existing Biden Administration policies for responsible AI and accompanying laws are ineffective at reigning in government actors like DHS.

Figure 1. DHS summary of key violations of existing AI policy and law.

- **DHS has not met basic transparency requirements for AI.** The OMB memo requires DHS to complete AI Impact Assessments (AIAs) *before* using any new AI technologies.[23] DHS has failed to publish any. Second, the DHS AI Inventory, which is required by statute, appears to be incomplete. For example, it fails to disclose long-time AI-powered technologies referenced in Section III.C and the Appendix of this report. Third, even where the AI tool is disclosed, the DHS AI Inventory contains skeletal or inaccurate information about how these technologies operate and/or their impact on communities. These findings were echoed by the Government Accountability Office which found that the DHS AI Inventory included multiple inaccuracies.[24]

- **There is no evidence that DHS is monitoring AI programs for real-time errors or civil rights violations, nor is it clear how DHS would define an error or violation.** Moreover, the agency has not stated how advocates or attorneys representing immigrants affected by inaccurate or unjust AI decisions can identify or rectify them.

- **DHS has failed to create a notification and redress process for people when it uses AI in a negative or adverse decision, such as denying someone asylum or release from detention.** It has also failed to establish a process for detecting and fixing when an AI program makes an erroneous or biased decision. These processes must be created for anyone impacted by the technology.

- **There is no way to know whether DHS is exempting its AI programs from following the rules for government use of AI.** DHS has not disclosed how it is waiving or exempting AI programs from the new safeguards, and whether it has reported them to OMB.[25]

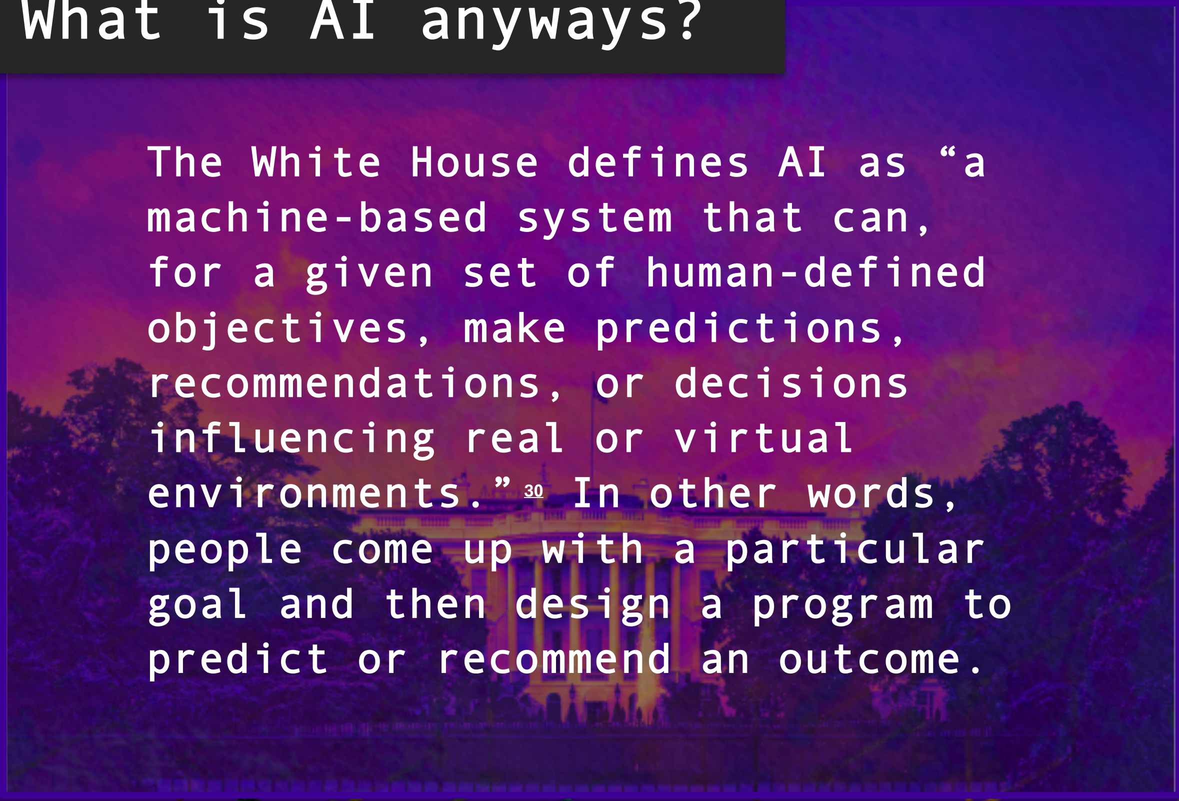
- **DHS has consistently failed to consult with impacted communities before creating AI products that can massively impact someone’s life** – for example, technologies that help decide whether someone remains in detention or obtains approval for a visa. DHS is using AI to assess eligibility, viability, or credibility of immigration benefit or relief claims, but there is no evidence that DHS followed requirements to “[c]onsult and incorporate feedback from affected communities and the public.”[26]

- **Communities who are subjected to DHS use of AI have no way to opt-out, even if the technology is inaccurate or discriminatory.** DHS has failed to “provide and maintain a mechanism for individuals to conveniently opt-out from the AI functionality in favor of a human alternative.”[27] Our research could not locate an opt-out method for any of the agency’s rights-impacting AI tools.

II. Background: Mythbusting Artificial Intelligence

This section covers some of the most common myths and concerns about AI. **AI programs are powerful, but just like the people who create them, they are neither "value neutral" nor objective.**[29] **Rather, AI can exacerbate existing discrimination. Moreover, it allows governments like DHS to hide their discriminatory policies and bypass due process rights by hiding behind flashy technology.** As explained below, it is far more difficult for immigrant communities and the larger public to know about and challenge automated bias in decision making.

What is AI anyways?



The White House defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments."[30] In other words, people come up with a particular goal and then design a program to predict or recommend an outcome.

AI does not eliminate discrimination; it can perpetuate and worsen it.

A growing number of studies, including studies by the government agency responsible for creating standards for AI,[31] recognize that AI has in many instances worsened discrimination.[32] One reason that this happens is because AI tools require a vast amount of data,[33] and the data is often biased. For example, when Amazon tested an AI tool to screen resumes and recommend applicants to the hiring team, the AI used data from the past ten years – data that showed that the majority of applicants had been men. Based on this data, the AI tool then recommended men's resumes more often.[34] The use of AI tools that are trained with biased data will most impact communities who already face discrimination.[35]

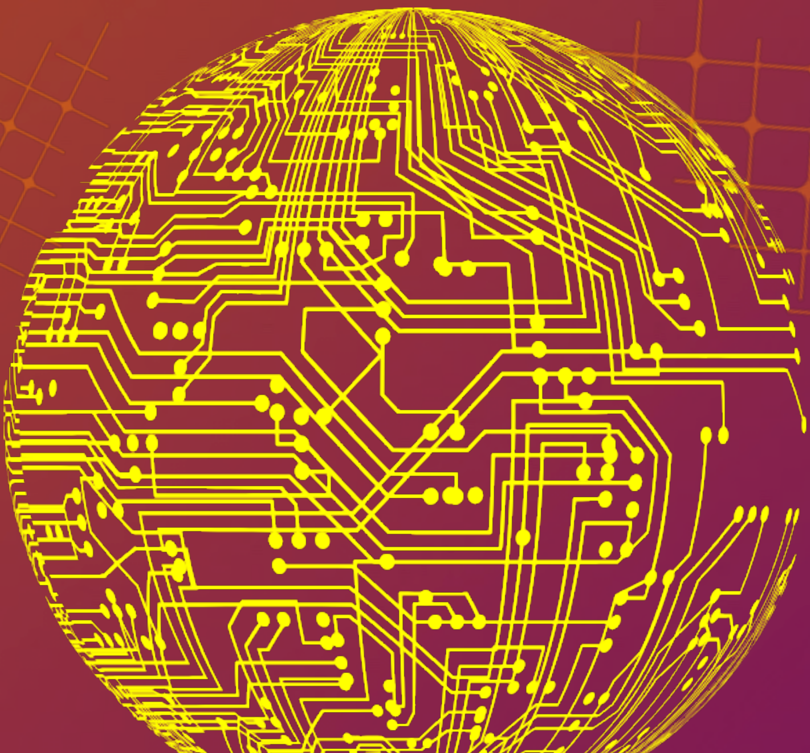
What is an algorithm?

An algorithm is a formula or list of rules that a human programmer sets out. This means that an algorithm is never a value neutral or objective decision maker; it always produces an outcome based on the goals and decisions of a human. An AI algorithm analyzes data in order to produce a certain outcome desired by its human programmer.

Another reason for AI discrimination is the human actors who create the algorithm or generate the data that trains the algorithm. Companies and the government can decide what factors and data the algorithm considers. Take the example of AI tools for predictive policing or threat assessment which are used to "predict" who and where crime will occur in the future. Often, companies create these AI tools based on historical crime data which is poisoned by the police's discriminatory targeting of Black and Brown people. Unsurprisingly, such AI tools have generally "predicted" that crime will happen in the same Black and Brown neighborhoods that historically experience high police presence and discriminatory policing.[36]

Studies have shown that predictive policing is wildly inaccurate – some tools have a success rate of less than half of a percent.[37] Why? **Because at the end of the day, an AI tool cannot be neutral because humans insert their own bias when they code the algorithm or because the data itself contains human bias.**

As one study puts it, "any...prediction will project the inequalities of the past into the future."[38] Concerningly, migration agencies such as USCIS are developing similar threat assessment tools to predict fraud, public safety and national security threats in immigration adjudications, as discussed in Section III.



DHS’s major goal for AI is to expand detention and deportation.

Concerns about AI go far beyond data bias and accuracy. As discussed in the previous section, the most troubling issue is often how human decision makers use AI to justify a policy or political goal.[39] In the context of immigration, DHS uses AI to make decisions about asylum, detention and deportation, which impact fundamental human rights. There are huge political pressures at DHS to restrict asylum, humanitarian relief, and other forms of immigration.[40] It is no surprise that most of the AI tools in the DHS AI Inventory are created for the purpose of immigration enforcement and criminalization. Regardless of how “accurate” the AI program is at recommending detention and deportation, in the hands of immigration and policing agencies, the technology furthers a fundamentally violent mission of targeting communities for detention and deportation.

AI technology is a black box that may mask discrimination and errors.

When we have no idea how an AI machine makes decisions, it is often referred to as a “black box” technology.[41] Black box is a scientific term that describes a system where one can see the input and the outcome, but not understand how or why the technology produces this outcome. AI is often a “black box” where its decision making process is unknown to the user and/or affected person.[42] For example, if an AI tool determines you are a public safety threat, you cannot examine the instructions or rationale behind why it made such a decision.

There are two core problems with black box technologies: (1) they allow their human creators to hide errors and bias, and 2) they undermine oversight and accountability because they make it impossible for the user and the public, such as communities who are directly impacted by these technologies, to understand what the government or corporation has programmed the technology to do.[43] That is, if people do not understand how or even know that a government agency has used an AI tool to make a decision, it becomes much more difficult to dispute the decision. Federal agencies will increasingly use AI to make decisions – from criminal sentencing and access to loans to health care and hiring decisions – making the disclosure of AI decision making critical to accountability.[44] Yet agencies rarely disclose their AI algorithms to the public, often deferring to corporations' claims that their algorithm is a trade secret.

AI is a surveillance marketing tool.

Corporations have exaggerated the power of artificial intelligence as they stand to gain huge profits from the sale of products that they can pass off as AI.[45] Federal agencies like DHS have touted AI as "the most consequential technology of our time."[46] However, it is important to recognize that AI is far from "magic".[47] In recent years, AI has come under increasing criticism. Researchers question whether it is scientifically possible for AI to make reliable decisions, now or ever.[48] For example, AI algorithms applied to legal writing have generated fake legal decisions when lawyers try to use them in legal briefs.[49] AI creators themselves do not seem to understand why or how their algorithms produce outcomes.[50] This technology remains largely untested, relies on mass harvesting people's personal data, and gives little consideration to human harms.[51]

III. Artificial Intelligence for DHS Decision Making

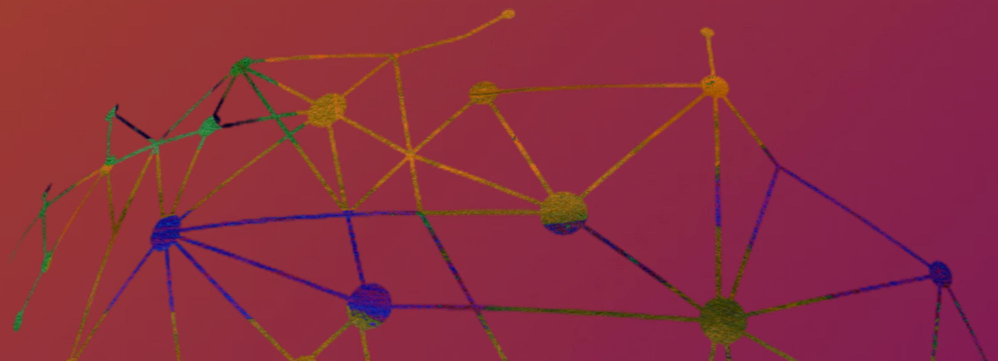
Determining an immigrant's eligibility for an immigration benefit or relief application can be a highly complex assessment by DHS officials. It involves DHS making fact-specific findings and analyzing multiple eligibility requirements and factors on discretionary relief. Adding an AI tool to this complicated adjudication process raises the serious risk of increasing erroneous and biased decision making by immigration officials.

Despite these red flags, DHS is plowing ahead with AI tools that automate decision making in the following areas:

- **Decisions on eligibility for an immigration benefit or relief.** Again, such determinations are complex factual and legal inquiries that an AI tool may have a hard time getting correct. For example, in the U.S. naturalization application, an AI could erroneously calculate the continuous presence requirement for an applicant, thereby leading to a denial or delay in their application;

- **Decisions of credibility and fraud.** Credibility and fraud determinations are made in the majority of immigration applications, particularly in asylum cases or deportation proceedings;

- **Decisions on whether someone is a public safety or national security threat.** For example, USCIS could deny DACA to an eligible person because they were arrested for an offense that the AI designates as making them a public safety threat.



> DHS's use of AI in decision making processes is highly alarming because of a long existing history of discriminatory decision making at the agency. There should be serious concern that any AI machine that USCIS creates could perpetuate and worsen existing discrimination.

We highlight a number of the agency's discriminatory practices here.

First, asylum seekers and other immigrants seeking immigration relief and benefits already face an immigration system rooted in anti-Black racism, arbitrary or inaccurate decision making, hostility and distrust of immigrants, and language access injustice. For example:

- **Anti-Black bias and Islamophobia in asylum applications:** there are wide disparities in the USCIS asylum system based on country of origin and religion, in which USCIS disproportionately denies asylum to Black and Muslim immigrants.[52]
- **Racial bias and Islamophobia in U.S. citizenship applications:** an empirical investigation of U.S. citizenship decisions, also known as naturalization decisions, by USCIS from 2014 to 2018 showed that, controlling for all other factors, USCIS is less likely to grant U.S. citizenship to Black, Latinx, and Muslim individuals, demonstrating clear inequality in citizenship decision making.[53]

- **Racial bias and Islamophobia in USCIS and/or DHS threat assessment:** USCIS and the larger immigration system disproportionately label Black, Brown, African and Muslim communities as national security, fraud, and public safety threats.[54]

- **Political and geographical bias in asylum decision making:** a data science study found that asylum relief grant rates in immigration court depended primarily on the political climate at the time and on the immigration judge, not on the merits of an individual's case.[55] Moreover, asylum grants radically vary based on geography, even though the average rate of denial is 70%. For example, asylum denial rates in parts of Texas, Georgia, Tennessee and Kentucky are higher than 95%,[56] with some judges denying 100% of cases.[57]

- **Language access injustice:** asylum seekers with limited English proficiency already face significant barriers to accessing asylum due to inaccessible or inadequate language services in the asylum process. For example, USCIS provides asylum seekers with limited language and interpretation services in all stages of the asylum process, from applying for an appointment to writing an application to conducting an interview.[58] In addition, asylum officers' language, cultural or linguistic biases during the asylum application and the credible fear determination processes can prevent someone from accessing asylum and other humanitarian protections.[59] The addition of AI into the process could worsen these barriers.

Second, recent research on AI bias in other contexts warrant serious caution around USCIS deployment of AI, particularly for fraud detection and threat assessment. **For example, AI tools created to detect fraud or plagiarism in the education context have been proven to have a clear bias against non-English speakers, consistently misclassifying non-native English writing samples as fraudulent.**[60] Since a large majority of immigrant applicants are limited English proficiency speakers, AI tools deployed to detect fraud in the USCIS context may be vulnerable to similar biases, leading to false positive detections of fraud.

Lastly, the immigration system and immigration law is highly complex. There is a chance that data tools built on these highly fact-specific data that apply complex legal requirements, case law analysis, discretionary findings, and legal judgments could produce erroneous results. Immigrants often have an immigration file with USCIS that is thousands of pages long. Take for example USCIS's failed attempt to digitize and categorize its own files. This seemingly basic task at USCIS uses an AI tool termed Evidence Classifier to categorize its files in the Electronic Information System (ELIS), the agency's internal case management system for immigration applications. For a period of 15 years, USCIS attempted to build ELIS and Evidence Classifier, experiencing multiple errors, failures and setbacks.[61] Based on this failure and the other examples of data system failures at DHS, there should be all the more concern that USCIS AI tools would produce error prone results in decision making.[62]

Despite the capability of such tools to impact millions of immigrants and U.S. families, these AI tools virtually operate in secret. USCIS has revealed close to no information about its AI algorithms. These AI tools threaten to automate USCIS's existing biases and inaccuracies at a scale never before experienced by immigrants, families, and their communities.

A. USCIS uses AI to make decisions on naturalization, asylum and withholding, and to help classify whether someone is a public safety or national security threat.

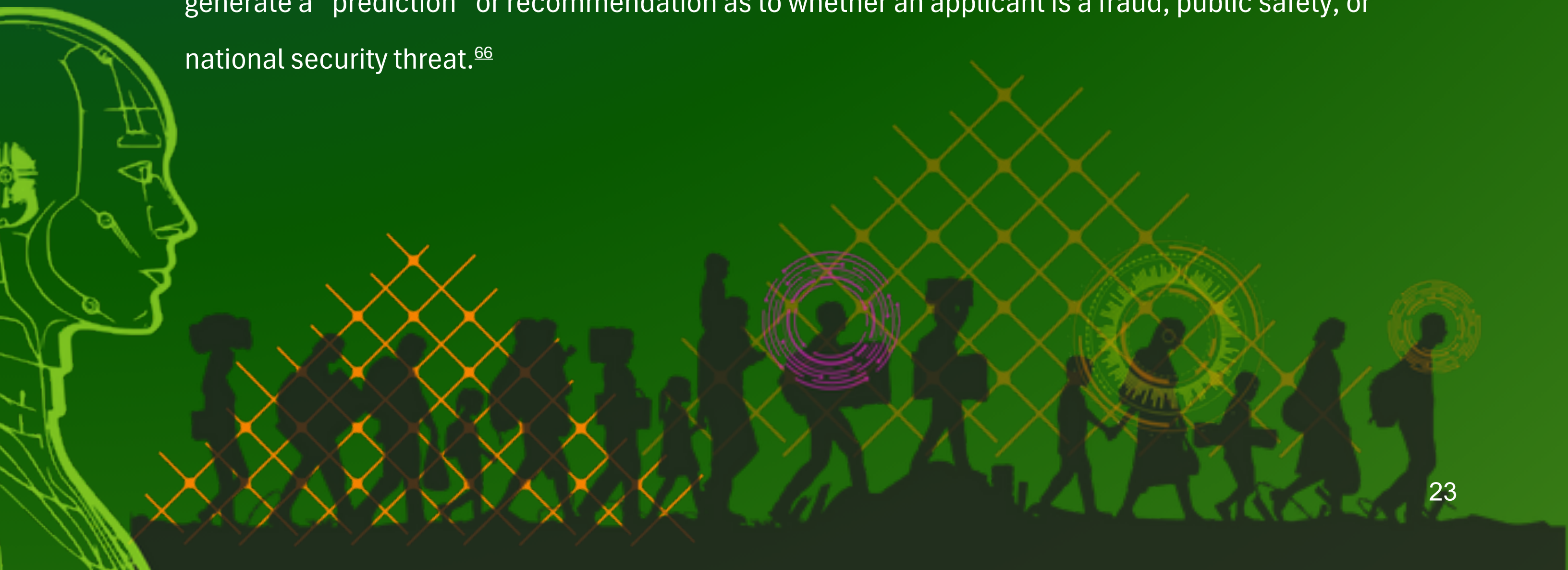
First, shockingly, USCIS already relies on AI to recommend decisions on U.S. naturalization applications and other immigration applications. Below are two examples:

- **Predicted to Naturalize** is an AI machine learning tool that screens naturalization applications to make predictions and recommendations on whether someone is eligible to naturalize. Naturalization law is incredibly complicated, especially when it comes to time eligibility or certain bars to eligibility – for example, whether certain conduct triggers the good moral character bar. USCIS provides no information on how this AI tool makes determinations around eligibility. As discussed above, USCIS has systematically discriminated against Black, Brown, Latinx and Muslim people in naturalization adjudications.[63] We are concerned about how the AI tool could make erroneous determinations and reproduce existing biases.

- **I-539 Approval Prediction** is an AI machine learning tool that USCIS is developing. The goal of the AI tool is to determine whether USCIS should approve an I-539 application, a visa extension application for students, travel, and H-1Bs. As discussed in Section III.B., questions arise as to how USCIS is training this AI machine to make determinations as to visa extension eligibility.

Second, USCIS uses AI to identify "fraud" in asylum and withholding applications. USCIS's Asylum Text Analytics (ATA) program claims to identify "plagiarism-based fraud" in asylum and withholding applications. The technology purportedly scans the narrative text of applications and looks for duplicate language repeated across applications. As the DHS AI Inventory explains, the Asylum Text Analytics program "employs machine learning and data graphing techniques to identify plagiarism-based fraud in applications for asylum status and for the withholding of removal by scanning the digitized narrative sections of the associated forms and looking for common language patterns."[64] Additionally, USCIS's Chief Technology Officer has stated that the agency's technologies flag "when applicants' stories don't align,"[65] indicating that the AI machine reviews an applicant's narrative not only individually, but also compared with other applicants' narratives. As discussed in the next Section, such a detection system that analyzes narrative language for fraud could be particularly susceptible to discrimination against limited English proficiency speakers, a large majority of asylum applicants.

Third, USCIS is developing an AI tool to detect fraud, public safety, and national security threats on a broader scale. The Fraud Detection and National Security (FDNS) Directorate operates a case management system termed the "Fraud Detection and National Security – Data System NextGen (FDNS-DS NextGen)" which USCIS officers use to screen a wide range of immigration applications for people with potential "fraud, public safety, or national security concerns." USCIS may soon introduce AI "predictive modeling" into FDNS-DS NextGen, meaning that this AI tool could conduct automated screenings of immigration applications in order to generate a "prediction" or recommendation as to whether an applicant is a fraud, public safety, or national security threat.[66]



The consequences of USCIS designating an immigrant as a fraud, public safety, or national security threat are huge. Such a determination could result in the denial of an otherwise meritorious immigration application, and lead to the denial of other forms of immigration relief and possibly deportation. For some immigrants, it can mean a life-time bar from the United States. Moreover, immigration fraud is a federal offense with up to a 10-year prison sentence.[67]

These three examples may only be the start of USCIS using AI tools to automate immigration application decision making and threat assessment. Concerningly, USCIS could expand the use of AI tools to other types of immigration benefit and relief applications with little oversight or accountability. For example, USCIS relies on AI to create large, searchable datasets on applicants, their associations, their immigration history, their biometrics, and more, which may be used for immigration decisions.[68] Additionally, DHS's recently published roadmap on AI announced that USCIS would be using ChatGPT to generate personalized legal training materials to USCIS refugee and asylum officers for use in eligibility interviews with immigrants.[69]

B. USCIS use of AI does not comply with federal responsible AI obligations, and should be suspended or terminated.

USCIS's AI programs described above, such as Predicted to Naturalize, Asylum Text Analytics, and FDNS-DS NextGen, raise a number of critical questions around bias and accuracy, and expose the failures of the agency to comply with basic AI obligations under the Biden Administration. Until these concerns are addressed and USCIS complies with these requirements, the agency should not use these AI tools.

USCIS has failed to provide the following information about its use of AI:

- **USCIS has failed to state what data it uses to train AI to identify "threats" or "plagiarism-based fraud."** For example, USCIS has not made it clear how its AI would distinguish between a normal baseline application and an application that contains a "common language pattern" that amounts to fraud.[70]

- **There is no evidence that USCIS is taking any steps to make sure that the ATA and FDNS-DS NextGen programs will not produce biased or discriminatory outcomes.** For example, it is unclear to what extent these programs flag immigrants as fraudulent or as national security threats on the basis of past USCIS discrimination targeting countries, regions or nationalities as a threat. How will the AI classify people from countries previously flagged by USCIS as having a high number of visa violators? Could the agency manipulate the AI algorithm to discourage immigration from certain countries due to purported "national security" or other impermissible political concerns?

- **It is unclear how the ATA program addresses language access bias, such as ensuring that the AI analyzes narratives from non-native English speakers without bias.** As mentioned earlier, AI tools created to detect plagiarism or fraud have been proven to be discriminatory particularly when used on non-native English speakers, leading decision makers to misclassify their written narratives as fraudulent.[71] In the immigration adjudication process, concerns around bias may be compounded by inadequate access to language services and an adjudicator's lack of cultural context.

- **USCIS does not appear to have any oversight mechanisms to monitor bias, accuracy, and impact of its AI machines before and after rollout. It is also unclear when in the USCIS adjudicatory process its AI machines are making recommendations or decisions.** If these machines engage in biased decision making on immigration applications, USCIS does not notify affected applicants and there is no process to seek redress against adverse AI decisions.

The answers to these questions could have wide ranging implications for how many applications are flagged as fraudulent, a public safety, or a national security threat. Unfortunately, USCIS has not met basic federal requirements for safeguarding responsible AI, and has not provided any answers on these questions. There are no Privacy Impact Assessments (PIA) for a number of the AI tools, let alone AI Impact Assessments (AIA).[72, 73] Moreover, USCIS does not notify affected applicants as to whether these AI tools have been used in negative decisions or allow applicants to contest those decisions. There is no way for applicants to opt-out or to choose a human USCIS adjudicator that does not use AI in their review of an application.

Furthermore, there is serious doubt whether DHS provides sufficient human oversight over the decisions of an AI tool after rollout. **Yet, even if an USCIS official reviews the decisions of the AI tool, that may not be a sufficient check.** First, just because someone reviews an AI decision does not mean that they would know if that decision by the AI was discriminatory or erroneous. Research shows that people are regularly incompetent at judging the quality or accuracy of information generated by algorithms, an issue termed "automation bias." This means that human oversight of AI can end up providing a false sense of security against AI harms.[74] Second, people have their own biases – whether they are aware of them or not – and they can use AI to justify unfair decision-making because the technology appears objective. For example, top-down policy priorities and high caseloads at USCIS may create pressure on officials to rely on AI tools to produce results, clear case quotas, or meet other policy goals.

Lastly, the lack of a notification mechanism informing an applicant that AI was involved in a derogatory determination raises procedural due process concerns because the applicant has no opportunity to review, much less challenge, the AI's decision.[75] USCIS is effectively requiring migrants to meet a standard on fraud, public safety and national security that is completely unknown, and an immigrant's failure to pass this machine's test could mean the denial of their application and a fraud, public safety or national security threat designation that may have additional immigration consequences.

In sum, USCIS falls short of implementing even basic safeguards against AI abuse. These USCIS AI programs operate as secret, black box machines. Given all these concerns, USCIS should not be able to deploy these AI tools. It is deeply troubling that USCIS has fast-tracked the adoption of AI technologies that impact major life-saving measures like asylum without community consultation and without disclosing what DHS has done to safeguard affected communities from AI's harms.

The recklessness under which USCIS has rolled out these AI tools is even more shocking when one considers the stakes for immigrants seeking immigration relief in the context of escaping violence and even death. Adding AI to the asylum and immigration adjudication process to screen and evaluate millions of applications could result in massive harm, automating racial bias and intensifying adjudication inaccuracies at a far larger scale than any human asylum officer.

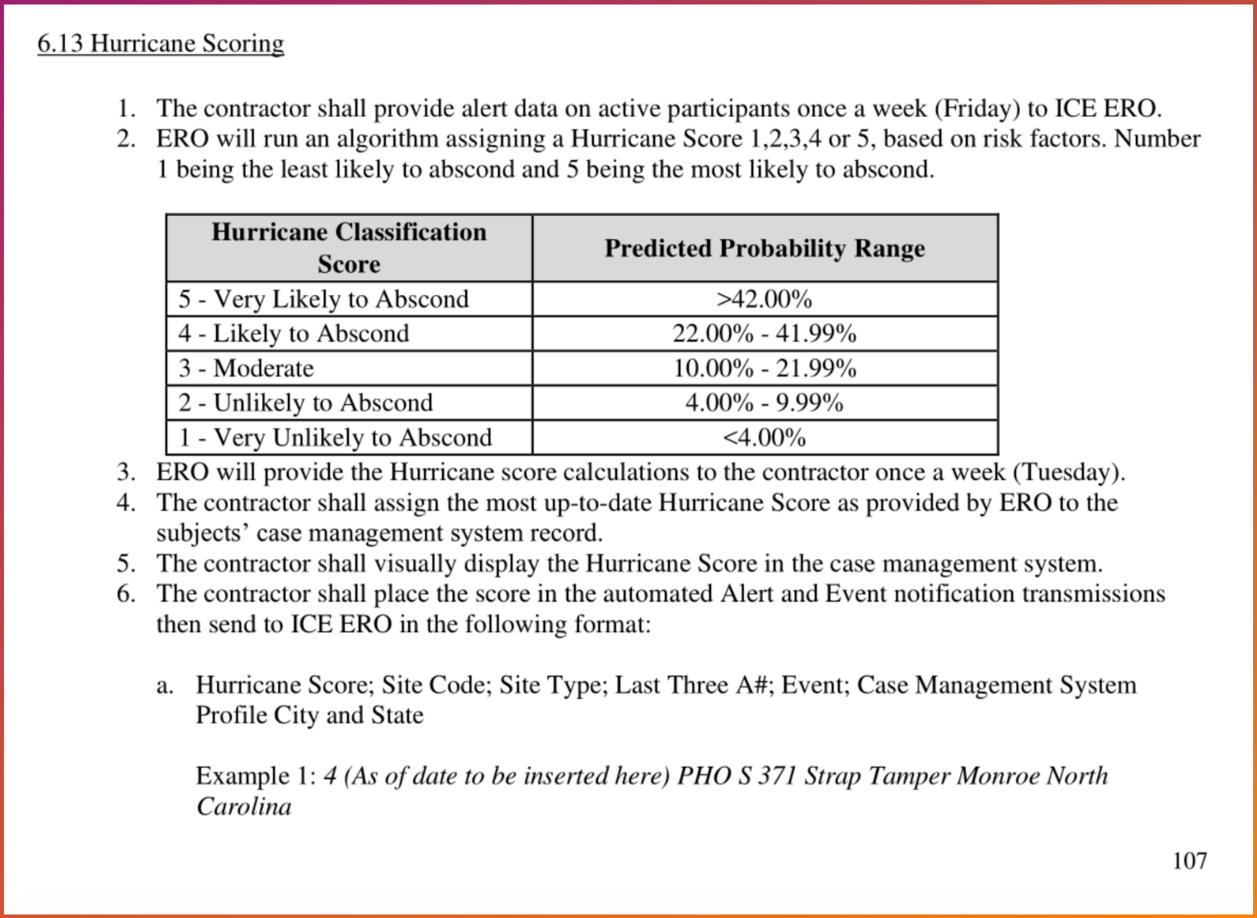
C. ICE uses AI to automate decision making on electronic monitoring, detention and deportation.

USCIS is not the only agency deploying AI to make critical decisions impacting immigrants and their families and communities in the US. Our research found that ICE and CBP also use AI to make critical life-impacting decisions about whether to detain or deport someone.

i. ICE runs a "Hurricane Score" AI tool for decisions on electronic surveillance.

ICE uses an artificial intelligence tool to inform decisions on an immigrant's terms of electronic monitoring, otherwise known as the Intensive Supervision Appearance (ISAP) program. The ICE ISAP program is an electronic monitoring program that subjects nearly 200,000 immigrants and families to location surveillance, facial recognition and voice recognition surveillance via GPS tracking devices and the SmartLINK cell phone app.[76] A FOIA lawsuit filed by Just Futures Law, Community Justice Exchange, and Mijente uncovered documents showing how ICE uses a predictive algorithm that generates a **"Hurricane Score"** on a weekly basis to make decisions on someone's conditions of supervision under ISAP. [77]

Figure 2: Documents obtained by Just Futures Law show ICE uses an AI tool to make decisions on electronic surveillance conditions for people subjected to the ISAP Program.



6.13 Hurricane Scoring

1. The contractor shall provide alert data on active participants once a week (Friday) to ICE ERO.
2. ERO will run an algorithm assigning a Hurricane Score 1,2,3,4 or 5, based on risk factors. Number 1 being the least likely to abscond and 5 being the most likely to abscond.

Hurricane Classification Score	Predicted Probability Range
5 - Very Likely to Abscond	>42.00%
4 - Likely to Abscond	22.00% - 41.99%
3 - Moderate	10.00% - 21.99%
2 - Unlikely to Abscond	4.00% - 9.99%
1 - Very Unlikely to Abscond	<4.00%

3. ERO will provide the Hurricane score calculations to the contractor once a week (Tuesday).
4. The contractor shall assign the most up-to-date Hurricane Score as provided by ERO to the subjects' case management system record.
5. The contractor shall visually display the Hurricane Score in the case management system.
6. The contractor shall place the score in the automated Alert and Event notification transmissions then send to ICE ERO in the following format:

   a. Hurricane Score; Site Code; Site Type; Last Three A#; Event; Case Management System Profile City and State

   Example 1: *4 (As of date to be inserted here) PHO S 371 Strap Tamper Monroe North Carolina*

107

According to limited FOIA records, ICE and its private contractor BI Inc. appear to run an algorithm on a weekly basis to predict someone's likelihood to "abscond," or not comply with its ISAP program. This Hurricane Score is likely used to inform and justify decisions around whether to subject someone to escalated forms of electronic monitoring.[78] The score is visually displayed in BI's case management system, and ICE receives automated alerts on the individual if and when the Hurricane Score changes.

Little information is known about ICE's Hurricane Score AI tool. The DHS AI Inventory does not mention this ICE AI tool and there is no Privacy Impact Assessment on it. There is no information on what risk factors ICE uses, how the AI analyzes these risk factors to predict a person's likelihood to abscond from ISAP, nor what data the AI machine is trained on.[79] ICE could be using this Hurricane Score classification system to justify keeping immigrants under high intensity ISAP surveillance, increasing their conditions of surveillance, or even re-detaining individuals.[80] Indeed, one of the major criticisms of the ICE ISAP program is that immigrants are subject to long periods of ISAP surveillance and that it is difficult to get ICE or BI officials to release individuals from the program even after years of compliance.[81]

ii. ICE uses the Risk Classification Assessment AI tool to increase immigrant detention.

ICE uses an AI tool termed the Risk Classification Assessment (RCA) to make decisions on the detention of immigrants. First developed by IBM[82] and rolled out in 2012, the RCA claims to assess an immigrant's level of "threat to the community" and "risk of flight" in order to make a decision about whether or not they should remain detained.[83] In its outdated 2012 Privacy Impact Assessment for the RCA, DHS stated that the RCA uses factors such as criminal justice information, disability status, substance abuse history, immigration history and case status, ties to the community, length of time at current address, the number of family members in someone's home, property information, employment and education information to make detention decisions. However, ICE has never revealed how the RCA analyzes these factors to produce a recommendation on "risk" and detention. In addition, the RCA is not included in the DHS AI Inventory.

Years of research and advocacy have exposed significant bias and politicized manipulation of the RCA AI tool. Studies show that over time, ICE has increasingly used the RCA to justify detaining migrants at higher and higher rates.[84]

For example, while the RCA initially included the option to recommend release, in 2015 and 2017, ICE stopped the algorithm from recommending release for anyone. In 2020, civil rights and civil liberties groups sued ICE over its use of the "rigged" RCA, claiming the RCA violated due process rights under the Fifth Amendment.[85] Practically, the RCA allows ICE to weaponize technology to maximize its goal of detaining as many immigrants as possible. It enables immigration officials to hide its biased decision making behind an AI tool's secret algorithm and the technology's veneer of neutrality.

In deploying ICE's Hurricane Score and Risk Classification Assessment tools, DHS has already sidestepped many of its obligations around responsible AI. Neither ICE nor CBP has met bare minimum safeguards around AI as required by the AI Executive Order, OMB memo, and accompanying law and policy. There are no AI Impact Assessments, no notification process that allows a person to know that the system was used, nor redress procedures to fix an error made by these systems. There has been no agency outreach to engage the public and affected communities around the impact of these AI tools. At this juncture, it is unclear which, if any, of these obligations DHS and its sub agencies will follow; we remain deeply concerned over the possibility of further civil rights and due process violations by ICE and CBP and how DHS plans to address them.

Particularly given that ICE has manipulated its RCA tool in the past to increase detention, these AI tools run the serious risk of intensifying bias and errors in the immigration system, and could be weaponized to justify the detention and deportation of millions of affected people. Given the large-scale abdication of these responsible AI obligations, DHS should suspend the use of these AI tools by December 1, 2024 as required under the OMB memo.

Conclusion: The Future of AI Means We Need DHS Accountability Now

Now more than ever, there is an urgent need for AI accountability mechanisms that do not allow DHS to shroud the technology that is at the core of its mission to detain, deport and tear apart immigrants, families and communities.

DHS has ambitious plans to swiftly expand AI. For example, USCIS now uses generative AI to generate training materials for asylum and refugee officers.[86] Corporations are arguing that AI translation tools can replace human translators for immigration proceedings despite clear indicators that these AI translators may not be able to assess culture or context critical to asylum or other immigration applications.[87]

DHS's next iteration of AI includes huge investments in an array of sensors – cameras, x-rays, and other technologies that surveil and analyze audio, video, social media, and biometric information (eye, iris, fingerprint, face, DNA) collected from millions of people who live in or transit through the United States.[88] At this very moment, electronic wrist shackles that monitor someone's location, like those used by ICE,[89] are one of the fastest growing carceral surveillance technologies.[90] Even robot dogs are beginning to utilize more and more AI.[91]

In sum, DHS has a massive amount of data at its disposal to create and train AI with little to no accountability.

DHS is not alone. Across the globe, migration agencies are testing AI lie-detection programs on migrants and relying on real-time AI biometric eye sensors, even though these AI tools are suspected to have significant error rates.[92]

Although a mountain of evidence exists showing that AI policing technologies worsen discrimination against Black, Brown and immigrant communities, AI development at DHS is moving at breakneck speed. Despite DHS's repeated promises to promote "responsible and trustworthy AI" and protect civil rights and privacy rights, DHS has ignored basic safeguard requirements of the Biden Administration. What has DHS done? It has published an AI roadmap that outlines its 2024 plans,[93] created multiple task forces composed largely of big tech, big corporations and private sector representatives,[94] and released an incomplete inventory of AI tools. These efforts contain little to no outreach to civil society or affected communities, no information about how the agency monitors or evaluates AI for civil rights violations, and no mechanisms for notification or redress. **It means the winners of the new AI regime are the corporations who profit off government contracts, now worth billions, to supercharge immigration policing, detention, and deportation.**

Particularly when mass detention, mass deportation and family separation of millions are at stake, our communities need more than lip service. They deserve action. DHS must terminate, or at the very least, suspend the use of these technologies by December 1, 2024. If the status quo on DHS AI deployment continues, it is blaring evidence that the Biden Administration's directives on AI are not nearly enough to hold DHS accountable for its use of surveillance technologies that can cause and worsen harm to communities.

Appendix: Other DHS Artificial Intelligence Tools

While this report focuses on AI for automated decision making, our research uncovered other alarming areas of DHS deployment of artificial intelligence – AI for processing sensitive and personal information about millions of people, AI for the deadly border wall, and AI for biometric surveillance. While the immigrant rights movement, journalists, and researchers have worked hard to expose a number of these technologies in recent years, these surveillance programs are now equipped and powered by artificial intelligence, increasing the power and danger of these technologies.

A. DHS uses AI for data processing in order to increase deportations

DHS relies on AI to amass, sort, and organize massive databases of information. DHS then uses this data for raids, deportations, and other enforcement activities. Below, we highlight a number of alarming AI processing tools that ICE and CBP use:

- **ICE's Repository for Analytics in a Virtualized Environment (RAVEn):** RAVEn is a $300 million program,[95] led by contractor Booz Allen Hamilton, which enables ICE to investigate and target immigrants by analyzing massive datasets and mapping associations between people.[96] RAVEn uses AI to correct data, analyze trends, and purportedly identify "criminal patterns" among surveillance datasets pulled from social media, biographic data, biometric data, and data on hundreds of millions of people culled from DHS databases. It is unclear what information informs the criteria for the AI to determine patterns of criminality within RAVEn. Using AI to clean, associate, and process complex data about someone could have real life harms. For example, the AI technology might identify someone's home address among a list of other addresses, leading ICE to conduct a raid at a location based on the AI machine's recommendation. We also have concerns as to whether RAVEn's AI tool accurately draws associations, links data sets, and identifies patterns for enforcement targeting. [97]

- **Giant Oak and Babel X for processing social media surveillance data:** CBP and ICE have spent millions on Giant Oak Search Technology (GOST), which monitors and analyzes data from social media and all over the internet, flagging supposedly "derogatory" content.[98] ICE and CBP have used these social media tools to inform decisions on immigration applications, surveil protests, track journalists and dissidents, and target Muslim communities.[99] GOST reportedly produces a red light suggesting agencies deny entry, or a green light ("no derogatory information unearthed"), for an applicant. Additionally, CBP and ICE have purchased AI-enabled Babel X, which allows agencies to screen social media posts, driver's license information, social security numbers, location information and more.[100]

- **Predictive automation used by DHS data brokers**: ICE has a $22.1 million contract with data broker LexisNexis which provides over 11,000 ICE agents access to data analytics tools that "automate" decisions about vetting, screening, and targeting people for deportation.[101] CBP has a $15.9 million contract with LexisNexis for access to troves of highly sensitive personal data, including facial recognition information and Babel X social media surveillance data, that the agency can use to track people throughout the U.S. and at the border.[102] LexisNexis does not only provide access to massive quantities of data pulled from thousands of government and commercial data sources, it also reportedly provides tools that it claims can analyze data, make predictions, and produce assessments about immigrants based on that data. For example, the LexisNexis contract states that the company will help ICE in “identifying potentially criminal and fraudulent behavior before crime and fraud can materialize.”[103] Once again, it is not clear what criteria LexisNexis uses to program the technology, nor how criminality or “fraudulent behavior” is defined or interpreted by the technology.

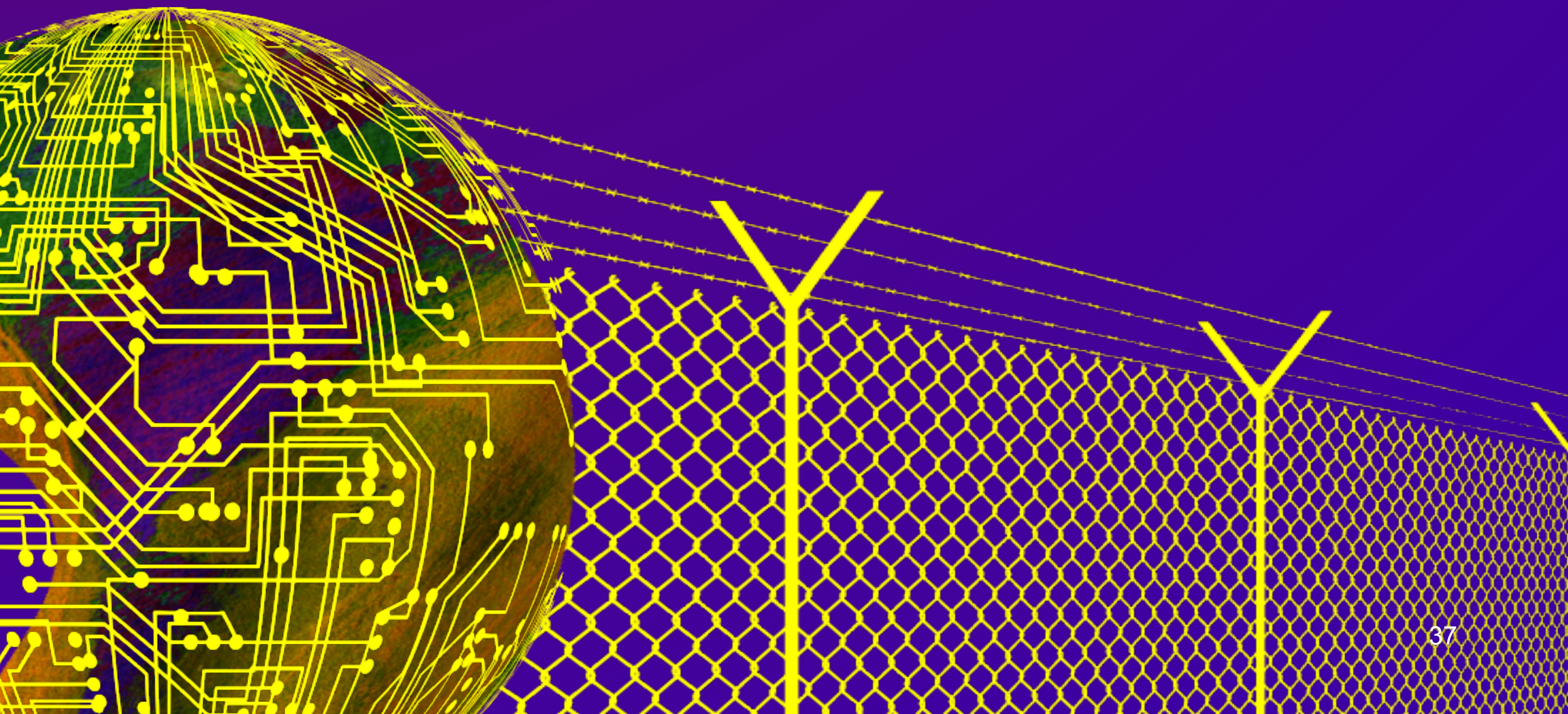
- **CBP’s Automated Targeting System (ATS):** Customs and Border Protection (CBP) uses the Automated Targeting System (ATS) to designate whether someone is a “suspected terrorist” or “high risk” in order to decide whether to grant an immigrant’s entry into the US.[104] ATS scans and cross-references data about an immigrant pulled from a variety of sources: law enforcement watch lists, airline records, border crossing data, Department of Motor Vehicle records, social media data, facial images, and over 10,000 commercial and government data sources sold by data broker LexisNexis.[105] Similar to the automated decision making tools at USCIS and ICE, ATS is a black box. We do not know what criteria or risk factors CBP uses to create and train the ATS tool to predict threats or what ATS deems as “suspect” or “high risk.”[106] As a result, someone may be subjected to increased inspection, denied boarding a plane, denied entry, have their visa revoked or worse based on ATS’s secret decision to assign a particular “threat” level to them.

While DHS use of AI for data processing may seem like a benign use case, this data is often extracted en masse and analyzed by AI to conduct enforcement – to target, criminalize, or separate people from their families. Even without AI, it is extremely alarming that agencies have nearly unlimited access to billions of highly personal, sensitive data points about hundreds of millions of people.[107] AI analysis of these huge datasets expands the detention and deportation machine.

B. AI is powering the deadly border wall

The digital border wall is made up of surveillance towers, ground sensors, aerial surveillance blimps, drones, biometric technologies such as facial recognition, and technologies that track people, phones, vehicles and property in real-time.[108] All together, these technologies create an environment of surveillance, control and death.

The digital border wall pushes migrants to take longer, more dangerous routes to avoid detection – leading to more deaths in the desert. Peer-reviewed research has shown that there is “significant correlation between the location of border surveillance technology, the routes taken by migrants, and the locations of recovered human remains in the southern Arizona desert.”[109] According to the United Nations, the U.S.-Mexico Border is the deadliest land route for migrants worldwide.[110] 2022 was the deadliest year on record for migrants, with the U.S. Border Patrol reporting finding the remains of more than 895 migrants who died along the U.S.-Mexico border.[111] That being said, multiple sources suggest that the U.S. Border Patrol consistently undercounts migrant deaths at the border, and community groups have in recent years identified death counts up to four times higher than the official government count in certain regions.[112,113]



Our research reveals that artificial intelligence now powers many CBP surveillance technologies that form this digital border wall. For example:

- **Autonomous Surveillance Towers:** DHS's $6 billion border surveillance tower project includes at least 200 towers that use AI, among over 450 total towers.[114] The AI-enabled towers sold by Anduril Industries carry out constant surveillance and use algorithms to detect and track the movement of people up to 1.7 miles away. Media reports suggest that CBP has a goal to "maximize" its use of AI to flag people crossing the border without authorization in real-time.[115]
- **AI for Autonomous Situational Awareness** is a video technology system with a motion sensor that snaps a series of photos as soon as it detects a vehicle and its direction.
- AI-enabled **Matroid technology** is used to analyze photo or video content to detect the presence of people as part of CBP's Automated Item of Interest Detection (ICAD) technology. Matroid is also used in CBP's RVSS Legacy Overhauled System Project (INVNT) to detect and continuously track people and objects in video streams sourced from hundreds of surveillance towers in rural and urban areas along the border.
- **Automated Ground Surveillance Vehicles, also known as robot dogs**: In 2022, Ghost Robotics contracted with DHS to deploy autonomous robot dogs on a pilot basis at the Southern Border.[116] The US military has contracted for robotic dog equipment from the same company[117] and has used a version of the same robot dog, stating that it is equipped with an AI-enabled digital imaging system that "can automatically detect and track people, drones, or vehicles, reporting potential targets to a remote human operator."[118] While our research could not confirm if the robot dogs used by DHS incorporate AI, it is possible that DHS will purchase AI-powered robot dogs in the near future, if it has not already.

C. DHS uses AI for biometric surveillance

DHS increasingly uses AI to conduct biometric surveillance, particularly facial recognition. There is growing evidence that facial recognition technology produces biased and inaccurate outcomes. For example, a 2019 federal government study found significantly higher false positives when facial recognition technology is deployed on Black and Asian individuals compared to white males.[119] Additionally, there have been a number of high profile cases of facial recognition false matches, leading to the wrongful arrest of Black individuals.[120]

Despite these civil rights and privacy concerns, a number of DHS sub-agencies continue to purchase and use AI-powered biometric surveillance:

- CBP subjects asylum seekers and many nonimmigrants to facial recognition via the **CBPOne app.**[121] CBP justifies this use of technology as a way to reduce "fraudulent activity" and increase order.[122] Asylum seekers must download the application and take a selfie to access CBP services, such as making an asylum appointment. The application's AI "liveness detection" claims to verify someone's identity based on their photo. The application is reproducing anti-Black bias: CBP has admitted fewer Black asylum seekers because the technology is not programmed to recognize dark-skinned people, according to nonprofit organizations working with asylum seekers at the U.S.-Mexico border.[123] Additionally, CBP uses the **Traveler Verification Service (TVS),** AI facial comparison technology, to verify the identity of people arriving or departing the U.S.[124]

- ICE buys facial recognition technology sold by controversial company **Clearview AI** to conduct immigration enforcement. Clearview AI is a company that has incurred substantive fines and penalties worldwide for non-consensual scraping of facial images.[125] Although Clearview AI engages in actions that violate the OMB memo, DHS continues to contract with the company.

- ICE requires immigrants to submit to facial recognition surveillance as part of their conditions of release from immigration detention. Nearly 160,000 immigrants are subject to **SmartLINK** mobile application surveillance under ICE's Intensive Supervision Appearance Program (ISAP).[126] This form of ISAP surveillance requires people to submit to frequent AI facial recognition in addition to location surveillance and voice verification via a mobile application on their phone.[127] In addition, ICE recently began tracking people in ISAP using the BI VeriWatch, a wrist-worn GPS tracking device that also uses facial recognition tech.[128] Evidence suggests that there are accuracy and bias issues with the facial recognition algorithm used by ICE.[129]

None of the AI tools raised in this Appendix are in compliance with the responsible AI requirements of President Biden's AI Executive Order or the OMB memo. Many of these AI tools were not even disclosed as part of the DHS AI Inventory. No AIA exists on these DHS facial recognition programs nor did DHS consult with impacted groups before releasing a face capture and recognition policy in 2023. This policy states that when facial recognition technologies are used for identity verification, they cannot be the "sole basis" for a denial of administrative action or a law enforcement action.[130] However, this DHS policy pertaining to facial recognition still does not comply with the subsequent Biden Executive Order or OMB memo. For example, it does not include a mechanism to address error, does not require notification of the person who receives an adverse action based in part on facial recognition technology, and does not provide an opt-out option for immigrants.

Endnotes

[1] Edward Graham, *Biden's $1.67 trillion budget boosts tech, AI,* NextGov, Mar. 11, 2024, https://www.nextgov.com/policy/2024/03/bidens-167-trillion-budget-boosts-tech-ai/394841/.

[2] *AI investment forecast to approach $200 billion globally by 2025,* Goldman Sachs (Aug. 1, 2023), https://www.goldmansachs.com/intelligence/pages/ai-investment-forecast-to-approach-200-billion-globally-by-2025.html.

[3] DHS is contracting with OpenAI, Anthropic, Meta, Microsoft, Google and Amazon to build and host its AI technologies. *See* Cecelia Kang, *The Department of Homeland Security Is Embracing A.I.,* N.Y. Times, Mar. 18, 2024, https://www.nytimes.com/2024/03/18/business/homeland-security-artificial-intelligence .html.

[4] *Department Of Homeland Security AI Roadmap 2024,* U.S. Dep't of Homeland Sec. (2024), https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf.

[5] Alejandro N. Mayorkas, *Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components,* U.S. Dep't of Homeland Sec. (Aug. 8, 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_139-06-acquistion-use-ai-technologies-dhs-components.pdf.

[6] *New Report on the Nation's Foreign-Born Population,* U.S. Census Bureau (Apr. 9, 2024), https://www.census.gov/newsroom/press-releases/2024/foreign-born-population.html.

[7] *Understanding Our Data,* U.S. Citizenship and Immigration Services (Dec. 2, 2020), https://www.uscis.gov/tools/reports-and-studies/understanding-our-data; *Naturalization Statistics*, U.S. Citizenship and Immigration Services (May 9, 2024), https://www.uscis.gov/citizenship-resource-center/naturalization-statistics.

[8] *Executive Office for Immigration Review Adjudication Statistics,* U.S. Dep't of Justice (Jan. 18, 2024), https://www.justice.gov/eoir/media/1344791/dl?inline.

[9] *FACT SHEET: Biden-Harris Administration Executive Order Directs DHS to Lead the Responsible Development of Artificial Intelligence,* U.S. Dep't of Homeland Sec. (Oct. 30, 2023), https://www.dhs.gov/news/2023/10/30/fact-sheet-biden-harris-administration-executive-order-directs-dhs-lead-responsible.

[10] The text of the Advancing American AI Act at Section (b) of Sec. 7224 states: "Not later than 180 days after the date of enactment of this Act— (1) the Secretary of Homeland Security....shall issue policies and procedures for the Department related to—(A) the acquisition and use of artificial intelligence; and (B) considerations for the risks and impacts related to artificial intelligence-enabled systems, including associated data of machine learning systems, to ensure that full consideration is given to— (i) the privacy, civil rights, and civil liberties impacts of artificial intelligence-enabled systems; and (ii) security against misuse, degradation, or rending inoperable of artificial intelligence-enabled

sys-tems…" Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7224(a), 7224(d)(1)(B), and 7225 (codified at 40 U.S.C. 11301 note), https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf.

11. Mayorkas, *supra* note 5, at 3.

12. *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* Exec. Office of the President (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. This EO builds on prior policies issued by the White House Office of Science and Technology Policy. *See, e.g., Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, White House Office of Science and Technology Policy (Oct. 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

13. The impacts the OMB is trying to mitigate are as follows: "Rights-Impacting AI" includes: "1. Civil rights, civil liberties, or privacy, including but not limited to freedom of speech, voting, human autonomy, and protections from discrimination, excessive punishment, and unlawful surveillance; 2. Equal opportunities, including equitable access to education, housing, insurance, credit, employment, and other programs where civil rights and equal opportunity protections apply; or 3. Access to or the ability to apply for critical government resources or services, including healthcare, financial services, public housing, social services, transportation, and essential goods and services." *See* Shalanda D. Young, *Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence,* Office of Management and Budget (Mar. 28, 2024), https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

14. *Id.* at 1.

15. *Id.* at 32.

16. *Id.* at 16-18.

17. Exec. Office of the President, *Exec. Order No. 13960: Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, 85 Fed. Reg. 78,939 (Dec. 8, 2020), https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

18. Young, *supra* note 13, at 24-25.

19. *Id.* at 12, 22.

20. "Agencies must provide and maintain a mechanism for individuals to conveniently opt-out from the AI functionality in favor of a human alternative, where practicable and consistent with applicable law and governmentwide guidance." *Id.* at 24.

21. *Id.* at 14, 16-17.

[22] Mayorkas, *supra* note 5.

[23] Young, *supra* note 13, at 17.

[24] Tom Temin, *DHS' list of AI use cases found inaccurate, GAO says,* Federal News Network, Feb. 28, 2024, https://federalnewsnetwork.com/artificial-intelligence/2024/02/dhs-list-of-ai-use-cases-found-inaccurate-gao-says/.

[25] Young, *supra* note 13, at 17.

[26] *Id.* at 22.

[27] *Id.* at 24. Although the opt-out requirement does not apply to fraud investigations, DHS has not yet provided a human alternative opt-out for any of its AI programs.

[28] Under the current AI framework, the civil rights agency within DHS, the Office for Civil Rights and Civil Liberties (OCRCL), does not carry the authority to constrain DHS or its sub-agencies from using harmful AI. The CAIO can permit the use of the AI program, even if OCRCL opposes.

[29] "Artificial intelligence systems use data we generate in our daily lives and as such are a mirror of our interests, weaknesses, and differences. Artificial intelligence, like any other technology, is not value-neutral." *See* Trustworthy & Responsible AI Resource Center, *The Language of Trustworthy AI: An In-Depth Glossary of Terms*, National Institute of Standards and Technology, U.S. Dep't of Commerce (May 13, 2024), https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary.

[30] Exec. Office of the Pres., *supra* note 12.

[31] *There's More to AI Bias Than Biased Data, NIST Report Highlights,* Nat. Inst. of Standards and Tech., U.S. Dep't of Commerce (Mar. 16, 2022), https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights.

[32] Brianna Scott, Jeanette Woods, Ailsa Chang, *How AI could perpetuate racism, sexism and other biases in society*, NPR, Jul. 19, 2023, https://www.npr.org/2023/07/19/1188739764/how-ai-could-perpetuate-racism-sexism-and-other-biases-in-society; Shin, D., Zaid, B., Biocca, F., Rasul, A., *In Platforms We Trust? Unlocking the Black-Box of News Algorithms through Interpretable AI*, Journal of Broadcasting & Electronic Media, 66(2), 235–256 (2022), https://doi.org/10.1080/08838151.2022.2057984.

[33] Cecilia Kang, Cade Metz, Stuart A. Thompson, *Four Takeaways on the Race to Amass Data for A.I.*, N.Y. Times, Apr. 6, 2024, https://www.nytimes.com/2024/04/06/technology/ai-data-tech-takeaways.html.

[34] Jeffrey Dastin, *Insight - Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters, Oct. 10, 2018, https://www.reuters.com/article/idUSKCN1MK0AG/.

35. Norori N, Hu Q, Aellen FM, Faraci FD, Tzovara A, *Addressing bias in big data and AI for health care: A call for open science*, Patterns (Oct. 8, 2021), 2(10): 100347, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8515002/.

36. *Before the Bullet Hits the Body: Dismantling Predictive Policing in Los Angeles*, Stop LAPD Spying Coalition (May 8, 2018), https://stoplapdspying.org/before-the-bullet-hits-the-body-dismantling-predictive-policing-in-los-angeles/; Aaron Sankin, Dhruv Mehrotra, Surya Mattu, Annie Gilbertson, *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, The Markup and Gizmodo, Dec. 2, 2021, https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

37. Aaron Sankin, Surya Mattu, *Predictive Policing Software Terrible At Predicting Crimes*, The Markup, Oct. 2, 2023, https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes.

38. Sandra G. Mayson, *Bias In, Bias Out*, The Yale Law Journal Vol. 128 No. 8 2124-2473 (June 2019), https://www.yalelawjournal.org/article/bias-in-bias-out.

39. Nat. Inst. of Standards and Tech., *supra* note 31.

40. *See e.g.* Camilo Montoya-Galvez, *U.S. to empower asylum officials to reject more migrants earlier in process*, CBS News, May 8, 2024, https://www.cbsnews.com/news/immigration-us-asylum-migrants-new-regulation/; *DHS Announces Proposed Rule and Other Measures to Enhance Security, Streamline Asylum Processing*, U.S. Dep't of Homeland Sec. (May 9, 2024), https://www.dhs.gov/news/2024/05/09/dhs-announces-proposed-rule-and-other-measures-enhance-security-streamline-asylum.

41. Lou Blouin, *AI's mysterious 'black box' problem, explained*, Uni. of Michigan-Dearborn News, Mar. 6, 2023, https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained.

42. Saurabh Bagchi, *Why We Need to See Inside AI's Black Box*, Scientific American, May 26, 2023, https://www.scientificamerican.com/article/why-we-need-to-see-inside-ais-black-box/.

43. Id.

44. Tom Simonite, *AI Experts Want to End 'Black Box' Algorithms in Government*, Wired, Oct. 18, 2017, https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/.

45. Julia Angwin, *Press Pause on the Silicon Valley Hype*, Opinion, N.Y. Times, May 15, 2024, https://www.nytimes.com/2024/05/15/opinion/artificial-intelligence-ai-openai-chatgpt-overrated-hype.html; Hasan Chowdhury, *It looks like it could be the end of the AI hype cycle*, Business Insider, Apr. 4, 2024, https://www.businessinsider.com/ai-leaders-worry-that-their-industry-is-based-on-hype-2024-4?op=1.

46. *Supra* note 4, *Dep't Of Homeland Sec. AI Roadmap 2024*, at 4.

47. Daniel Howley, *AI snake oil is here, and it's a distraction*, Yahoo Finance, Jun. 21, 2023, https://finance.yahoo.com/news/ai-snake-oil-is-here-and-its-a-distraction-151024678.html; Tony Ho Tran, *How Congress Fell for Sam Altman's AI Magic Tricks*, The Daily Beast, Sep. 29, 2023, https://www.thedailybeast.com/how-congress-fell-for-openai-and-sam-altmans-ai-magic-tricks.

48. Gebru, T., & Torres, Émile P. *The Tescreal bundle: Eugenics and the promise of utopia through artificial general intelligence*, First Monday, 29(4), (2024), https://doi.org/10.5210/fm.v29i4.13636; Angelina Wang, Sayash Kapoor, Solon Barocas, Arvind Narayanan, *Against Predictive Optimization: On the Legitimacy of Decision-Making Algorithms that Optimize Predictive Accuracy,* Journal of Responsible Computing (2023), https://predictive-optimization.cs.princeton.edu/.

49. Matthew Dahl, Varun Magesh, Mirac Suzgun, Daniel E. Ho, *Hallucinating Law: Legal Mistakes with Large Language Models are Pervasive,* Stanford Human-Centered Artificial Intelligence (Jan. 11, 2024), https://law.stanford.edu/2024/01/11/hallucinating-law-legal-mistakes-with-large-language-models-are-pervasive/; Eric Hysen, *Use of Commercial Generative Artificial Intelligence (AI) Tools*, U.S. Dep't of Homeland Sec. (Oct. 24, 2023), https://www.dhs.gov/sites/default/files/2023-11/23_1114_cio_use_generative_ai_tools.pdf.

50. Chloe Xiang, *Scientists Increasingly Can't Explain How AI Works*, Vice News, Nov. 1, 2022, https://www.vice.com/en/article/y3pezm/scientists-increasingly-cant-explain-how-ai-works.

51. Daxia Rojas, *AI Relies on Mass Surveillance, Warns Signal Boss*, Barrons, May 23, 2024, https://www.barrons.com/news/ai-relies-on-mass-surveillance-warns-signal-boss-20280d0a.

52. *US Discrimination Against Black Migrants, Refugees and Asylum Seekers at the Border and Beyond*, Human Rights First (Aug. 8, 2022), https://humanrightsfirst.org/library/cerd-us-discrimination-against-black-migrants-refugees-and-asylum-seekers-at-the-border-and-beyond/; *Pretense of Protection: Biden Administration and Congress Should Avoid Exacerbating Expedited Removal Deficiencies*, Human Rights First (Aug. 2022), https://humanrightsfirst.org/wp-content/uploads/2023/01/PretenseofProtection-21.pdf; *USCIS Records Reveal Systemic Disparities in Asylum Decisions*, Human Rights First (May 2022), https://humanrightsfirst.org/wp-content/uploads/2022/09/AsylumOfficeFOIASystemicDisparities.pdf; Giselle Rhoden, Nicole Chavez, *Black immigrants are more likely to be denied US citizenship than White immigrants, study finds,* CNN, Feb. 24, 2022, https://www.cnn.com/2022/02/23/us/black-immigrants-citizenship-approval-disparities/index.html; Emily Willingham, *U.S. Records Reveal Bias Against Muslim and Black Citizenship Applicants*, Scientific American, Mar. 15, 2022, https://www.scientificamerican.com/article/u-s-records-reveal-bias-against-muslim-and-black-citizenship-applicants.

53. Leslie Ridgeway, *Data study uncovers inequities in U.S. naturalization adjudication process*, USC Gould School of Law (Feb. 23, 2022), https://gould.usc.edu/news/data-study-uncovers-inequities-in-u-s-naturalization-adjudication-process/; Emily Ryo, Reed Humphrey, *The importance of race, gender, and religion in naturalization adjudication in the United States*, PNAS Vol. 119 No. 4 (Feb. 22, 2022), https://www.pnas.org/doi/10.1073/pnas.2114430119.

[54] Spencer Reynolds, José Guillermo Gutiérrez, Melanie Geller, *Little Change in Biased, Ineffective DHS Countering Violent Extremism Program,* Brennan Center for Justice (Feb. 27, 2024), https://www.brennancenter.org/our-work/research-reports/little-change-biased-ineffective-dhs-countering-violent-extremism-program; *Muslim Ban Fact Sheet*, ACLU (2017), https://www.aclu.org/sites/default/files/field_document/muslim_ban_fact_sheet.pdf; Cynthia Gonzalez, *Discriminatory and Illegal Practices Administered in the United States' Discretion When Employing the National Security Exception to Claim Inadmissibility of Syrian Refugees for Resettlement,* Uni. of Miami Nat'l Sec. & Armed Conflict Law Review (2015), https://repository.law.miami.edu/umnsac/vol6/iss1/12; *Muslims Need Not Apply: How USCIS Secretly Mandates the Discriminatory Delay and Denial of Citizenship and Immigration Benefits to Aspiring Americans*, ACLU SoCal (August 2013), https://www.aclusocal.org/sites/default/files/carrp-muslims-need-not-apply-aclu-socal-report.pdf; Penn State Law Immigrants' Rights Clinic and Rights Working Group, *The NSEERS Effect: A Decade of Racial Profiling, Fear, and Secrecy,* Center for Immigrants' Rights Clinic Publications (2012), http://elibrary.law.psu.edu/irc_pubs/11; *Under the Radar: Muslims Deported, Detained and Denied on Unsubstantiated Terrorism Allegations,* Center for Human Rights and Global Justice, NYU, Asian American Legal Defense and Education Fund (2011), https://perma.cc/VK8G-S8AJ.

[55] "[W]hether the EOIR grants asylum to an applicant or not depends in majority on the combined effects of the political climate and the individual variability of the presiding judge — not the individual merits of the case," *See* Vyoma Raman, Catherine Vera, CJ Manna, *Bias, Consistency, and Partisanship in U.S. Asylum Cases: A Machine Learning Analysis of Extraneous Factors in Immigration Court Decisions,* EAAMO '22: Proceedings of the 2nd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (Oct. 17, 2022), https://dl.acm.org/doi/10.1145/3551624.3555288.

[56] *Know Your Court: Place is Important*, Free Migration Project (2022), https://freemigrationproject.org/wp-content/uploads/2022/07/FMP-asylum-denial-flyer-5.pdf.

[57] *Judge Bruce Imbacuan, FY 2017 - 2022, Houston Immigration Court*, Transactional Records Access Clearinghouse (Oct. 26, 2022), https://trac.syr.edu/immigration/reports/judge2022/00778HOU/index.html; *Asylum Success Varies Widely Among Immigration Judges*, Transactional Records Access Clearinghouse (Dec. 9, 2021), https://trac.syr.edu/immigration/reports/670/.

[58] Leila Lorenzo, Laura Wagner, Ariel Koren, Juan Camilo Mendez, *CBP One's obscene language errors create more barriers for asylum seekers*, Respond Crisis Translation (Apr. 1, 2024), https://respondcrisistranslation.org/en/newsb/cbp-ones-obscene-language-errors-create-more-barriers-for-asylum-seekers; Melissa Wallace, Carlos Iván Hernández, *Language Access for Asylum Seekers in Borderland Detention Centers in Texas*, Journal of Language and Law 143-156 (Dec. 2017), https://www.researchgate.net/publication/322732710_Language_Access_for_Asylum_Seekers_in_Borderland_Detention_Centers_in_Texas.

[59] Jeremy A. Rud, *Asylum Text Analytics as an Algorithmic Silver Bullet: The Impossible Quest for Automated Fraud Detection*, Talking Politics, Jun. 20, 2023, https://talkingpoliticsonline.blogspot.com/2023/06/asylum-text-analytics-as-algorithmic.html; Diana Eades, *Applied Linguistics and Language Analysis in Asylum Seeker Cases,* Applied Linguistics, Vol. 26, Iss. 4 (Dec. 1, 2005), https://academic.oup.com/applij/article-

abstract/26/4/503/145244?redirectedFrom=fulltext; Marie Jacobs, Katrijn Maryns, *Managing narratives, managing identities : language and credibility in legal consultations with asylum seekers*, Language in Society (2022), https://biblio.ugent.be/publication/8697923; Jeanette L. Shroeder, *The Vulnerability of Asylum Adjudications to Subconscious Cultural Biases: Demanding American Narrative Norms*, B.U. Law Review (2017), https://www.bu.edu/bulawreview/files/2017/03/SCHROEDER.pdf.

60. Weixin Liang, Mert Yuksekgonul, Yining Mao, Eric Wu, James Zou, *GPT detectors are biased against non-native English writers*, Patterns Vol. 4 Iss. 7 (Jul. 10, 2023), https://arxiv.org/abs/2304.02819.

61. *Evidence Classifier,* Am. Council for Tech. and Indus. Advisory Council (Oct. 2022), https://www.actiac.org/et-use-case/evidence-classifier; Hana Schank, Tara Dawson McGuinness, *What Happened When the U.S. Government Tried to Make the Immigration System Digital*, Slate, Apr. 16, 2021, https://slate.com/technology/2021/04/elis-uscis-digital-immigration-system.html ("[s]even years into development, the first design of the system—ELIS 1—was such a dysfunctional mess that USCIS was forced to scrap it and start again. Another four years and a total $1 billion later, the USCIS had managed to digitize just two out of the 94 forms.")

62. *Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy*, U.S. Gov't Accountability Office (Sept. 12, 2023), https://www.gao.gov/products/gao-23-105959.

63. Ridgeway, *supra* note 53.

64. *Artificial Intelligence Use Case Inventory*, U.S. Dep't of Homeland Sec., https://www.dhs.gov/data/AI_inventory, (last accessed May 31, 2024).

65. Dave Nyczepir, *USCIS automating pre-processing of immigration cases,* Fedscoop, Apr. 15, 2021, https://fedscoop.com/uscis-automating-immigration-pre-processing/.

66. DHS has published conflicting information about the stage of development for FDNS-DS NextGen and its AI programs. In the DHS AI Use Case Inventory, DHS states that FDNS-DS NextGen is in the "Initiation" stage of system development life cycle. In contrast, in the DHS AI Use Case Inventory Library, DHS states that FDNS-DS NextGen is in the "Operation and Maintenance" stage of system development life cycle, suggesting that DHS may already be operating this program with new AI technologies. This inconsistency provides additional evidence of DHS' overall lack of transparency and failed accountability around its use of AI. *Compare supra* note 64 *with Artificial Intelligence Use Case Library,* U.S. Dep't of Homeland Sec. (Apr. 11, 2024), https://www.dhs.gov/publication/ai-use-case-inventory-library.

67. A number of immigration statutes, regulations, and policies on immigration relief or benefits contain statutory or discretionary exclusions related to public safety, national security, and fraud. *See*, e.g., 8 USC § 1182(a)(6)(C)(i) (fraud and willful misrepresentation ground of inadmissibility); 8 U.S.C. § 1158(b)(2)(A)(iv) (asylum bar for being a danger to the security of the U.S.); 8 U.S.C. § 1231(b)(2)(B)(iv) (same); *Memorandum from Alejandro N. Mayorkas, Sec'y of Homeland Security, Guidelines for the Enforcement of Civil Immigration Law* (Sept. 30, 2021), available at https://www.ice.gov/doclib/news/guidelines-civilimmigrationlaw.pdf (last visited Feb. 9, 2024) (designating those who

public safety or national security threats as priorities for removal); 8 CFR § 236.22(b)(6) (posing a threat to national security or public safety is a bar to DACA). Immigrants can be sentenced up to 10 years of prison for a first time offense of making a false statement with respect to a material fact in any application, affidavit, or other document required by the immigration laws or regulations. *See* 18 U.S. Code § 1546(a).

68. *See e.g. supra* note 64 (USCIS's Identity Match Option (IMO) Process with DBIS Data Marts and Person-Centric Identity Services A-Number Management Model).

69. *See supra* note 4, at 12; *see also* "Large Language Models for an Officer Training Tool," *supra* note 64 ("The tool will generate dynamic, personalized training materials that adapt to officers' specific needs…")

70. *See* Rud, *supra* note 59. Jeremy Rud sets out a number of these algorithm concerns in further detail, e.g. "does 'boilerplate language'—which USCIS has named as a main concern—obviously amount to plagiarism? And what other "patterns or anomalies" constitute fraud according to USCIS? Anomalies for whom, and against what background assumptions about how a "normal" application ought to look and how a story of persecution should be told?"

71. Tara García Mathewson, *AI Detection Tools Falsely Accuse International Students of Cheating*, The Markup, Aug. 14, 2023, https://themarkup.org/machine-learning/2023/08/14/ai-detection-tools-falsely-accuse-international-students-of-cheating,

72. We could not locate a DHS PIA for the Asylum Text Analytics system. Conducting Privacy Impact Assessments and Privacy Threshold Assessments are the bare minimum that USCIS is required to do under the Privacy Act. This is another indication of lack of accountability and failure at DHS to meet the most basic privacy compliance requirements when it comes to artificial intelligence. Our research did reveal another PIA for the "Pangea Text" program which describes a similar and equally troubling algorithm programmed to flag "fraud" and "national security" concerns in the narrative section of asylum applications. Concerningly, the Pangea Text tool is not only used by USCIS but also ICE. As the PIA explains, ICE can access Pangea Text for "investigatory and immigration court functions," suggesting that ICE agents may be able to use the algorithm for deportation efforts. *See Privacy Impact Assessment for the Pangaea: Pangaea Text,* U.S. Dep't of Homeland Sec. (Jan. 6, 2021), https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis085-pangea-january2021_0.pdf.

73. The Privacy Impact Assessment for FDNS-DS has not been updated with new information around FDNS-DS NexGen. *See Privacy Impact Assessment for Fraud Detection and National Security Directorate*, U.S. Dep't of Homeland Sec. (updated Mar. 3., 2020) https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis013-01fdnsprogram-appendixgupdate-march2020.pdf.

74. Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, Comput. Law & Sec. Review, Vol. 45 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3921216; Lauren Leffer, *Humans absorb bias from AI–and keep it after they stop using the algorithm*, Scientific American, Oct. 2023, https://www.scientificamerican.com/article/humans-absorb-bias-from-ai-and-keep-it-after-they-stop-using-the-algorithm/.

[75] Crawford, Kate and Schultz, Jason, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, Boston College Law Review, Vol. 55, No. 93 (2013), https://ssrn.com/abstract=2325784.

[76] *Alternatives to Detention (ATD)*, Transactional Records Access Clearinghouse (May 4, 2024), https://trac.syr.edu/immigration/detentionstats/atd_pop_table.html.

[77] *CJE et al v. ICE et al*, Case No. 22-cv-02328 (N.D. Cal. 2023), https://www.justfutureslaw.org/iceatdfoia.

[78] Immi. and Customs Enforcement, Statement of Work, at 38, https://www.law.berkeley.edu/wp-content/uploads/2022/05/2022-12-09_ISAP-FOIA_ICEProduction3_ISAP4-SectionCStatementOfWork.pdf (BI Statement of Work obtained from FOIA lawsuit).

[79] Additionally, according to this chart, ICE labels people as Hurricane 5 (very likely to abscond) where the algorithm generates a probability of greater than 42% of absconding. In other words, ICE will designate a person as a Hurricane 5 even when the algorithm itself predicts that someone has a less than 50% chance of absconding.

[80] Based on conversations with ICE, researchers, and immigration advocates in 2023 and 2024, there is a chance that ICE may be using the ICE RCA AI tool discussed below at Section III.B.ii in part to generate the Hurricane Score. However, because there is little information around the algorithm that ICE uses to generate the Hurricane Score, we could not confirm this. As discussed in the subsequent section, the ICE RCA tool has serious biases, and is heavily weighted towards recommending detention over release. If the Hurricane Score AI tool significantly adopts the RCA algorithm, it would likely be similarly rigged.

[81] *Tracked and Trapped: Experiences from ICE Digital Prisons*, African Bureau for Immigration and Social Affairs (ABISA), Boston Immigration Justice and Accountability Network (BIJAN), Community Justice Exchange, Detention Watch Network, Envision Freedom Fund, Freedom for Immigrants, Georgia Latino Alliance for Human Rights (GLAHR), Just Futures Law, La Resistencia, Long Beach Immigrant Rights Coalition (LBIRC), Mijente, Organized Communities Against Deportations (OCAD), and Youth Justice Coalition (May 2022), https://notechforice.com/digitalprisons.

[82] Aly Panjwani, *Rigged by Design: A glimpse at how ICE manipulates its algorithm to incarcerate immigrants strengthens the case for abolishing immigration detention*, Inquest, Oct. 29, 2021, https://inquest.org/rigged-by-design/.

[83] *Privacy Impact Assessment Update for the Enforcement Integrated Database (EID) Risk Classification Assessment (RCA 1.0), ENFORCE Alien Removal Module (EARM 5.0), and Crime Entry Screen (CES 2.0),* U.S. Dep't of Homeland Sec. (Apr. 6, 2021), https://www.dhs.gov/sites/default/files/publications/PIA%20EID%20Update%20for%20RCA_EARM%205_CES%202%2020120406%20FINAL%20%5BSigned%5D.pdf.

[84] Mark L. Noferi, Robert Koulish, *The Immigration Detention Risk Assessment*, Georgetown Immigration Law Journal 45 (2014), https://ssrn.com/abstract=2635247; Peter Henderson, Mark Krass, *Algorithmic Rulemaking vs. Algorithmic*

Guidance, Harvard Journal of Law & Technology, Vol. 37, No. 1 (2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4784350.

85. Adi Robertson, *ICE rigged its algorithms to keep immigrants in jail, claims lawsuit*, The Verge, Mar. 3, 2020, https://www.theverge.com/2020/3/3/21163013/ice-new-york-risk-assessment-algorithm-rigged-lawsuit-nyclu-jose-velesaca.

86. U.S. Dep't of Homeland Sec., *supra* note 4, at 12.

87. Yeganeh Torbati, *Google Says Google Translate Can't Replace Human Translators. Immigration Officials Have Used It to Vet Refugees*, ProPublica, Sept. 26, 2019, https://www.propublica.org/article/google-says-google-translate-cant-replace-human-translators-immigration-officials-have-used-it-to-vet-refugees.biddle

88. U.S. Dep't of Homeland Security Science & Technology Directorate, *Foundation Models at the Department of Homeland Security: Use Cases and Considerations*, U.S. Dep't of Homeland Sec. (April 2023), https://www.dhs.gov/sites/default/files/2023-12/23_1222_st_foundation_models_dhs_paper.pdf.

89. *ICE begins testing wrist-worn GPS monitoring technology*, U.S. Dep't of Homeland Sec. (Apr. 24, 2023), https://www.ice.gov/news/releases/ice-begins-testing-wrist-worn-gps-monitoring-technology.

90. *ICE Increases Use of GPS Monitoring for Immigrants in Alternatives to Detention (ATD)*, Transactional Records Access Clearinghouse (Mar. 15, 2024), https://trac.syr.edu/whatsnew/email.240315.html.

91. *Robot dogs and artificial intelligence will make borders safer, but what about privacy?*, Vogon Today, Dec., 2023, https://www.vogon.today/economic-scenarios/robot-dogs-and-artificial-intelligence-will-make-borders-safer-but-what-about-privacy/2023/12/15/.

92. *See* Bircan, T., Korkmaz, E.E. *Big data for whose sake? Governing migration through artificial intelligence*. Humanit Soc Sci Commun 8, 241 (2021). https://doi.org/10.1057/s41599-021-00910-x; Adam Tanner, *How Companies Are Using Artificial Intelligence to Tell if You're Lying*, Consumer Reports, Nov. 9, 2021, https://www.consumerreports.org/electronics/artificial-intelligence/how-companies-use-artificial-intelligence-to-detect-lying-a4041224738/.

93. U.S. Dep't of Homeland Sec., *supra* note 4.

94. Dimitri Kusnezov, Eric Hysen, *Artificial Intelligence Task Force (AITF) 90 Day Update*, U.S. Dep't of Homeland Sec. (Feb. 14, 2024), https://www.dhs.gov/sites/default/files/2024-05/24_02_14_sec_signed_ai_task_force_memo_508.pdf.pdf.

95. Chris Cornillie, *DHS Plans $300 Million Law Enforcement Data Analytics Platform*, Bloomberg Government, Apr. 20, 2021, https://about.bgov.com/news/dhs-plans-300-million-law-enforcement-data-analytics-platform.

96. *Award Profile Contract Summary: U.S. Dep't of Homeland Sec. (DHS) and Booz Allen Hamilton Inc.*, USASpending.Gov (2024), https://www.usaspending.gov/award/CONT_AWD_70CTD022FR0000002_7012_GS35F386DA_4732.

97. Additionally, RAVEn hosts an AI tool, the Mobile Device Analytics, that analyzes cell phone data. Like the other AI technologies, this tool allows analysts to analyze data and build associations for targeting. For example, this might look like churning through a cell phone's photo library or social media accounts and building profiles based on what the AI identifies in photos and videos.

98. Joseph Cox, *Inside ICE's Database for Finding 'Derogatory' Online Speech*, 404 Media, Oct. 24, 2023, https://www.404media.co/inside-ices-database-derogatory-information-giant-oak-gost/.

99. Faiza Patel, *Homeland Security's Intelligence Overreach: Two Cases Illustrate Risks to Civil Society*, Just Security, Mar. 8, 2019, https://www.justsecurity.org/63116/dhs-surveillance-reveals-oversight/; Faiza Patel, Rachel Levinson-Waldman, Raya Koreh, Sophia DenUyl, *Social Media Monitoring*, The Brennan Center for Justice (Mar. 11, 2020), https://www.brennancenter.org/our-work/research-reports/social-media-monitoring.

100. Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees,* Vice, May 17, 2023, https://www.vice.com/en/article/m7bge3/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees?ref=404media.co; *ICE seemingly inflated its contract with a cellphone location-tracking data broker to work around a "commercial data pause"*, Jack Poulson (Oct. 6, 2023), https://jackpoulson.substack.com/p/ice-seemingly-inflated-its-contract.

101. *Award Profile Contract Summary: U.S Dep't of Homeland Sec. (DHS) and LexisNexis Risk Solutions Inc.,* USASpending.Gov (2024), https://www.usaspending.gov/award/CONT_AWD_70CMSD21C00000001_7012_-NONE-_-NONE-; Sam Biddle, *LexisNexis Is Selling Your Personal Data to ICE So It Can Try to Predict Crimes,* The Intercept, Jun. 20, 2023, https://theintercept.com/2023/06/20/lexisnexis-ice-surveillance-license-plates.

102. Sam Biddle, *LexisNexis Sold Powerful Spy Tools to U.S. Customs and Border Protection*, The Intercept, Nov. 16, 2023, https://theintercept.com/2023/11/16/lexisnexis-cbp-surveillance-border/.

103. Biddle, *supra* note 101.

104. *DHS/CBP/PIA-006 Automated Targeting System*, U.S. Dep't of Homeland Sec. (May 2022), https://www.dhs.gov/publication/automated-targeting-system-ats-update.

105. *Privacy Impact Assessment Update for the Automated Targeting System, DHS/CBP/PIA-006(e)*, U.S. Dep't of Homeland Sec. (Jan. 13, 2017), https://www.dhs.gov/sites/default/files/2022-07/privacy-pia-cbp006-ats-july2022_0.pdf.

106. *Id.*; *see also DHS Privacy Office 2019 Data Mining Report to Congress,* U.S. Dep't of Homeland Sec. (Dec. 2, 2020), https://www.dhs.gov/sites/default/files/publications/2019_data_mining_report_final_12-2-20.pdf.

107. *How Data Brokers Assist ICE in Cook County,* Mijente and Just Futures Law (2023), https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/65283e83622fff1ee8837590/1697136260425/Final+Cook+County+Fact+Sheet+and+Graphic+2.pdf.

108. *The Deadly Digital Border Wall*, Mijente, Just Futures Wall and No Border Wall Coalition (2021), https://notechforce.com/wp-content/uploads/2021/10/Deadly.Digital.Border.Wall_.pdf.

109. Samuel Norton Chambers, et al., *Mortality, Surveillance and the Tertiary "Funnel Effect" on the U.S.-Mexico Border: A Geospatial Modeling of the Geography of Deterrence,* Journal of Borderland Studies, Vol. 36 (Jan. 31, 2019), https://www.researchgate.net/publication/330786155_Mortality_Surveillance_and_the_Tertiary_Funnel_Effect_on_the_US-Mexico_Border_A_Geospatial_Modeling_of_the_Geography_of_Deterrence.

110. *US-Mexico Border World's Deadliest Migration Land Route,* International Organization for Migration (Sept. 12, 2023), https://www.iom.int/news/us-mexico-border-worlds-deadliest-migration-land-route.

111. Gaby Del Valle, *Surveillance has a body count,* The Verge, Mar. 20, 2024, https://www.theverge.com/2024/3/20/24106098/cbp-migrant-deaths-border-surveillance.

112. *CBP Should Improve Data Collection, Reporting, and Evaluation for the Missing Migrant Program*, U.S. Gov't Accountability Office (Apr. 2022), https://www.gao.gov/assets/gao-22-105053.pdf; Bob Ortega, *Border Patrol failed to count hundreds of migrant deaths on US soil,* CNN, May 15, 2018, https://www.cnn.com/2018/05/14/us/border-patrol-migrant-death-count-invs/index.html; *El Paso Sector Migrant Death Database*, El Paso Sector Migrant Death Database (2024), https://www.elpasomigrantdeathdatabase.org/wp-content/uploads/2024/03/El-Paso-Sector-Migrant-Death-Database.pdf.

113. The Missing Migrants Project reports 370 migrant deaths at the US-Mexico border in 2023, noting that this count is incomplete and lacks an official count from US federal government sources. *370 Missing Migrants Recorded in North America*, Missing Migrants Project (2024), https://missingmigrants.iom.int/region/americas?region_incident=4076&route=3936&year%5B%5D=11681&incident_date%5Bmin%5D=&incident_date%5Bmax%5D=.

114. Daniel Boguslaw, *U.S. Government Seeks "Unified Vision of Unauthorized Movement,"* The Intercept, Mar. 12, 2024, https://theintercept.com/2024/03/12/dhs-border-towers-ai/; Dave Maas, *CBP Is Expanding Its Surveillance Tower Program at the U.S.-Mexico Border–And We're Mapping It*, Electronic Frontier Foundation (Mar. 20, 2023), https://www.eff.org/deeplinks/2023/03/cbp-expanding-its-surveillance-tower-program-us-mexico-border-and-were-mapping-it.

115. Monique O. Madan, *The Future of Border Patrol: AI Is Always Watching,* The Markup, Mar. 22, 2024, https://themarkup.org/news/2024/03/22/the-future-of-border-patrol-ai-is-always-watching.

116. James Vincent, *The US is testing robot patrol dogs on its borders,* The Verge, Feb. 3, 2022, https://www.theverge.com/2022/2/3/22915760/us-robot-dogs-border-patrol-dhs-tests-ghost-robotics; *Feature*

Article: Robot Dogs Take Another Step Towards Deployment at the Border, U.S. Dep't of Homeland Sec. Science and Tech. Directorate (Feb. 1, 2022), https://www.dhs.gov/science-and-technology/news/2022/02/01/feature-article-robot-dogs-take-another-step-towards-deployment.

117. *See, e.g., Award Profile Contract Summary: U.S. Dep't of Defense and Ghost Robotics Corp*., USASpending.Gov (2024), https://www.usaspending.gov/award/CONT_AWD_FA700023P0083_9700_-NONE-_-NONE-.

118. Benj Edwards, *Robot dogs armed with AI-aimed rifles undergo US Marines Special Ops evaluation,* Ars Technica, May 8, 2024, https://arstechnica.com/gadgets/2024/05/robot-dogs-armed-with-ai-targeting-rifles-undergo-us-marines-special-ops-evaluation/; *Ghost Robotics Vision 60*, U.S. Dep't of Defense (2020), https://www.defense.gov/Multimedia/Photos/igphoto/2002547643/. Vision 60 is the robot dog used by DHS.

119. Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use,* The Washington Post, Dec. 19, 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

120. Dave Gershgorn, *Black teen barred from skating rink by inaccurate facial recognition,* The Verge, Jul. 15, 2021, https://www.theverge.com/2021/7/15/22578801/black-teen-skating-rink-inaccurate-facial-recognition; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match,* N.Y. Times, Dec. 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; Kashmir Hill, *Wrongfully Accused by an Algorithm,* N.Y. Times, Jun. 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Elisha Anderson, *Controversial Detroit facial recognition got him arrested for a crime he didn't commit*, Detroit Free Press, Jul. 10, 2020, https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/; Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match,* N.Y. Times, Aug. 6, 2023, https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

121. U.S. Customs and Border Protection, *Agency Information Collection Activities; Revision; Arrival and Departure Record and Electronic System for Travel Authorization (ESTA),* Federal Register (Feb. 26, 2024), https://www.federalregister.gov/documents/2024/02/26/2024-03772/agency-information-collection-activities-revision-arrival-and-departure-record-and-electronic-system.

122. Dep't of Homeland Sec., *supra* note 64; *Fact Sheet: Using CBP One™ to Schedule an Appointment,* U.S. Customs and Border Protection (2023), https://www.cbp.gov/sites/default/files/assets/documents/2023-Jan/CBP%20One%20Fact%20Sheet_English_3.pdf.

123. Melissa Del Bosque, *Facing Bias: CBP's Immigration App Doesn't Recognize Black Faces, Barring Thousands from Seeking Asylum,* The Border Chronicle, Feb. 7, 2023, https://www.theborderchronicle.com/p/facing-bias-cbps-immigration-app; *United States of America: Mandatory Use of CBP One Application Violates the Right to Seek Asylum,* Amnesty International (May 7, 2023), https://www.amnesty.org/en/documents/amr51/6754/2023/en/. The racism

embedded in the CBPOne App raises concerns that other uses of facial matching technology by CBP may similarly be used to deny entry or freedom of movement to Black and Brown travelers.

124. *Supra* note 64.

125. *See e.g.* Complaint, *Renderos et al v. Clearview et al*, Case No. RG21096898 (County of Alameda Superior Ct. Dec. 16, 2022); Tonya Riley, *Feds' spending on facial recognition tech expands, despite privacy concerns,* Cyberscoop, Jan. 10, 2022, https://cyberscoop.com/feds-spending-on-facial-recognition-tech-continues-unmitigated-despite-privacy-concerns/; Natasha Lomas, *Clearview fined again in France for failing to comply with privacy orders*, TechCrunch, May 10, 2023, https://techcrunch.com/2023/05/10/clearview-ai-another-cnil-gspr-fine/.

126. Transactional Records Access Clearinghouse, *supra* note 90.

127. *Tracked and Trapped*, *supra* note 81.

128. *Biometric Facial Comparison: Unlocking New Opportunities in Community Corrections*, BI (Feb. 21, 2023), https://bi.com/biometric-facial-comparison-community-corrections/; *Wrist-Worn GPS Monitors Now Fastest Growing Electronic Monitoring Type Used by ICE,* Transactional Records Access Clearinghouse (May 14, 2024), https://trac.syr.edu/whatsnew/email.240514.html.

129. *Tracked and Trapped*, *supra* note 81; *Fact Sheet on ICE FOIA Lawsuit: ICE Documents Reveal Alarming Scale of Surveillance in ISAP Program,* Just Futures Law, Community Justice Exchange and Mijente (2023), https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/6512da273ccb7321c334ab6c/1695734312687/ATDFOIAFinal.pdf.

130. *Use of Face Recognition and Face Capture Technologies,* U.S. Dep't of Homeland Sec., at 6 (Sept. 11, 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.