BRENNAN
CENTER
FOR JUSTICE

DHS AT 20: AN AGENDA FOR REFORM

Overdue Scrutiny for Watch Listing and Risk Prediction

Reining In Civil Liberties Abuses and Assessing Efficacy

By Rachel Levinson-Waldman and José Guillermo Gutiérrez

PUBLISHED OCTOBER 19, 2023

The Department of Homeland Security (DHS) touches the lives of all Americans — U.S. citizens and lawful permanent residents — who board a plane, cross the border into Canada or Mexico, or seek a visa for a loved one to visit the United States.[1] DHS is likely the largest single U.S. government consumer — and creator — of detailed, often intimate information about individuals' lives. It stores the data it amasses in vast, interlocking databases to be recycled for purposes far beyond those for which it is initially collected.[2] The systems that house and analyze this data largely determine who is allowed to travel into and out of the country and how they are treated when they arrive.

This report addresses two categories of screening, vetting, and risk assessment efforts.[3] The first comprises programs that check travelers against watch lists and other databases of individualized, assertedly derogatory information.[4] The second consists of programs that identify travel patterns and other behaviors ostensibly related to terrorist or criminal activity and flag for scrutiny individuals whose activity matches those patterns.

Fundamental defects plague each of these types of programs. Vague standards draw in people with no connection to terrorism — overwhelmingly Muslims, people of color, and persons of Middle Eastern and South Asian descent. Records are riddled with factual errors. The programs operate without adequate privacy, civil rights, and civil liberties protections and have been used to target political activities protected by the First Amendment. Compounding these problems, the government's attempts to assess their efficacy have been superficial at best.

As it enters its third decade, DHS, along with other agencies and Congress, must evaluate how these programs function, determine whether they contribute measurably to national security, reckon with their effects on marginalized communities, tailor them to meet objective standards, and demonstrate empirical proof of success commensurate with the resources poured into them. Otherwise, they will continue to operate in a faulty and discriminatory manner that undermines core American values, with scant evidence that they contribute substantially to national security.

Watch Lists

The Terrorist Screening Database (TSDB), often referred to simply as the terrorist watch list, has served since 2004 as the government's main repository of information about individuals categorized as known or suspected terrorists.[5] As of June 2017, about 1.2 million individuals — including 4,600 Americans — were on the TSDB.[6]

Although the TSDB is maintained by the Threat Screening Center (TSC),[7] which is managed by the FBI and comprises multiple federal agencies, DHS uses the database as a cornerstone of its screening and vetting efforts. Federal law enforcement and intelligence agencies nominate individuals to the watch list on the basis of nonpublic watch-listing guidance.[8] Nominations must include information sufficient to identify the person being nominated and a minimum level of derogatory information to explain why they are being nominated.[9] For individuals with an asserted connection to international terrorism, agencies across the federal government send nominations to the National Counterterrorism Center (NCTC), an entity within the Office of the Director of National Intelligence.[10] For individuals asserted to have links solely to domestic terrorism, the FBI manages the nomination process.[11] All nominations are sent to the TSC, which accepts almost every nomination, inscribing the person in the TSDB.[12]

The Transportation Security Administration (TSA), a DHS component, manages and implements lists derived from the TSDB, including the No Fly and Selectee Lists, which it uses to screen airline passengers.[13] As the name suggests, people on the No Fly List are barred from flying to or from the United States, as well as over U.S. airspace or on U.S. airline carriers. People on the Selectee List are permitted to fly but are subjected to enhanced screening before boarding an aircraft, which may include physical searches of the traveler and their luggage and chemical tests for traces of explosive residue.[14]

Customs and Border Protection (CBP), another DHS component, also uses the TSDB to facilitate screening and vetting of travelers by analysts at its National Targeting Center (NTC) and by CBP Officers at ports of entry who may refer watch-listed individuals to secondary inspection.[15] During secondary inspection, agents may pull people aside for intrusive questioning, search their luggage, seize their phones or computers, or download and analyze data from their electronic devices.[16] A traveler's presence on the watch list is automatically grounds to subject their phone or laptop to an "advanced search," which involves reviewing, copying, and analyzing the device's contents.[17]

Local sheriff's offices and police departments may use TSDB data as well in determining whom to stop, and data is routinely shared with — and received from — foreign partners.[18] The process for populating the TSDB and its subsidiary lists and the ways the lists have been deployed raise a host of concerns.

Slippery Standards and Inadequate Vetting

To start, the category of "suspected terrorist" is nebulous and susceptible to broad interpretation based on subjective judgments. A suspected terrorist is defined as someone who is "reasonably suspected to be engaging in, has engaged in, or intends to engage in conduct" that constitutes terrorist activity or that is "in preparation for, in aid of, or related to" terrorist activity.[19] As a Virginia federal district court observed, because the NCTC guidance does not articulate what kind of conduct is "in aid of" or "related to" terrorism, it is "not difficult to imagine completely innocent conduct" forming the basis for "a string of subjective, speculative inferences that result in a person's inclusion" in the database. Such conduct could include a journalist reporting on terrorism, a devout Muslim "providing financial support to a charitable organization," or even a graduate student studying Arabic abroad.[20]

Furthermore, the multiple layers of review in the nomination process offer a "veneer of objectivity" that lends the watch lists greater credibility than is warranted.[21] The NCTC largely defers to nominating agencies' designations,[22] and the TSC has historically accepted nearly every nomination it receives from the NCTC and the FBI.[23] The nominating agencies are required to annually review their nominations of Americans to the TSDB, and the TSC is required to biannually review all Americans on the TSDB, the No Fly List, and the Selectee List. Details about the depth or scope of these reviews are not publicly available, however.[24] Overall, it seems that the TSC mainly confirms that procedural steps have been followed rather than assessing the accuracy of the underlying information or judgments.[25] And DHS's Office of Intelligence and Analysis (I&A), which formally serves as the department's watch-listing lead, has weak leverage over the other DHS monitoring components, increasing the risk that the components may not comply with the guidance in practice.[26]

This diffusion of responsibility means that no agency is held accountable for the rigor of nominations. Meanwhile, the various agencies have explicit and implicit reward systems for making nominations as well as institutional interests in emphasizing the prevalence of national security threats to ensure an ever-expanding flow of resources.[27] Taken together, this structure has created what a former director of the NCTC's Directorate of

Terrorist Identities has called a "zero-tolerance approach" by which the TSDB grows ever larger for fear of missing a potential risk, no matter how slight.[28]

Errors and Bloat

What scarce information has been released about the TSDB and its subsidiary lists portrays a system rife with inaccuracies. A 2007 audit by the Department of Justice's inspector general found that nearly 40 percent of the records examined contained "errors or inconsistencies."[29] A report two years later echoed those findings, determining that 35 percent of watch list records contained outdated information and that the FBI sometimes failed to remove people from the TSDB as required by its own policy.[30] A 2014 report — the last publicly available review of the TSDB — found that after the attempted "underwear bombing" in 2009, the TSC had added people to the list in bulk because of their connections to five undisclosed countries without meeting the required standard of individualized suspicion.[31] While the FBI bears responsibility for these failures, DHS agents routinely act on the information that resulted.

Furthermore, leaked versions of the TSDB and the No Fly and Selectee Lists show that they have swelled to a size that calls into question whether they are reasonably tailored to national security risks. In 2023, a Swiss hacker group obtained a 2019 version of the No Fly List that contained more than 1.5 million entries (likely representing fewer individuals in light of aliases and spelling permutations), along with a version of the Selectee List from the same year with more than 250,000 entries.[32] Data exposed online in 2021 contained 1.9 million records that appeared to be compiled from the TSDB.[33] A bloated watch list produces far more alerts than agents can respond to, accustoming them to false alarms and reducing the likelihood that they will recognize genuine threats.[34]

Mistaken nominations propagate through government databases, making the errors almost impossible to correct. In 2014, a federal judge found that a Malaysian PhD candidate at Stanford University had been put on the No Fly List erroneously and that the error had been replicated across multiple databases, resulting in the revocation of her visa. The court ordered the government to strike her from the list.[35] In 2017, FBI agents surveilled and raided the home of Ashraf Maniar, a U.S. citizen born and raised in California. Maniar had been subjected to enhanced inspection at airports and barred from boarding flights for years because of his friendship with a woman whom British police had arrested on terrorism charges and his humanitarian efforts in war-torn Syria.[36] Even after he succeeded in getting his name removed from the No Fly List, he apparently remained on the TSDB, which led to four days of detention and interrogation by Pakistan's Inter-Services Intelligence agency when he visited family in Karachi in 2020.[37] Maniar's wife was also placed on the No Fly List, evidently due in part to her relationship with Maniar, and other watch listees have alleged that their family members and associates have been placed on the watch list or subjected to additional scrutiny because of their associations.[38]

Religious Targeting

The watch lists disproportionately harm Muslims, including U.S. citizens.[39] While nominations are not supposed to be based solely on a candidate's race, ethnicity, religious affiliation, national origin, or First Amendment–protected activity, this sensitive information can be used if accompanied by other factors.[40] The Council on American-Islamic Relations (CAIR) analyzed the leaked 2019 No Fly and Selectee Lists and concluded that nearly 100 percent of the records on both lists corresponded to Muslim names,[41] with more than 10 percent of the records on the No Fly List containing the name Muhammad.[42] It appears that the list triggered the Secret Service to deny Mohamed Khairullah, a Muslim American citizen and the long-time mayor of Prospect Park, New Jersey, entrance to a 2023 Eid dinner at the White House.[43]

Being on a watch list can also trigger invasive questioning during travel, including about religious practices and other constitutionally protected matters. In March 2022, together with 20 other American Muslims, Abdirahman Aden Kariye, the imam at a Minnesota mosque, filed suit against DHS challenging their treatment at the border. Although Kariye, who became a U.S. citizen after fleeing Somalia as a child, does not know with certainty whether he is on one of the watch lists, his treatment every time he flies has led him to suspect that he is. This treatment has included being referred to secondary inspection and being subjected to questions by CBP officers about his religious beliefs and practices, such as "What type of Muslim are you?" and "What type of Islamic lectures do you give?"[44]

Naidal El-Takach, a U.S. citizen who joined Khairullah in a September 2023 lawsuit challenging the watch list, has experienced similar questioning. CBP and FBI officials at airports reportedly questioned El-Takach about his religious beliefs, including "whether he is Sunni or Shia Muslim, whether his wife wears hijab, whether he attends Islamic religious ceremonies, whether he performs daily prayers, and whether he attends Friday Jumu'ah services at his local mosque."[45] As a result, he stopped attending religious services.[46]

These allegations echo complaints lodged a decade earlier with DHS's Office for Civil Rights and Civil Liberties (CRCL) charging that CBP officers had "engaged in inappropriate questioning about religious affiliation and practices during border screening."[47] CRCL opened an investigation in 2011 but suspended it the following year when the CAIR Michigan chapter brought suit on behalf of different plaintiffs challenging the religious questioning of Muslims at the border.[48]

Downstream Consequences of the TSDB

>> The TSDB is used for purposes beyond border security. Agencies throughout the federal government share information from the database among themselves and with thousands of state and local police departments, which then feed information back into it.[49] Enlisting police in gathering personal information encourages pretextual stops and unwarranted surveillance. Government documents also indicate that of the interactions that local police report as being with watch-listed individuals, only a small fraction actually involve people on the watch list, suggesting a high rate of erroneous matches.[50] Saadiq Long, a U.S. Air Force veteran with no criminal record, sued the Oklahoma City Police Department in January 2023 after he was repeatedly pulled over within several months' time, "interrogated, handcuffed twice, and arrested at gunpoint."[51] One officer who stopped Long had received an automatic license plate alert that Long's vehicle was "under suspicion for a terrorist watchlist."[52] In response to the lawsuit, the department in 2023 instructed its officers not to use watch list status as the sole basis for stopping motorists.[53] Yet that directive seems unlikely to end Long's troubles: his watch list status has already impeded him from flying to visit his ailing mother or obtaining a truck driving license, and it led to his detention by Turkish officials.[54]

Identifying information from watch lists is apparently widely distributed beyond law enforcement as well. People who suspect that they are on a watch list have reported significant interference with basic financial transactions, including banking and money transfer services.[55] One U.S. citizen, Ibrahim Awad, was informed in 2016 by a sales associate at a car dealership that his name appeared on a watch list and that he had to be cleared by the FBI before he could test-drive a car.[56] Periodic leaks of watch list data and other sensitive information also demonstrate that the federal government struggles with confining disclosures to permitted recipients.[57] And watch-listed individuals have reported that the FBI has coercively offered to remove them from the list if they become informants and report on members of their communities.[58] The acknowledgment by a federal district court judge in 2017 that dissemination "may be so widespread that it is tantamount to public disclosure" and the observation by a former FBI special agent in 2014 that the watch-listing system was "revving out of control" thus remain salient today.[59]

No Proof of Effectiveness

Given these problems, a full assessment of the watch lists' value is overdue. Any such assessment would need to comprehensively evaluate the watch lists' efficacy and the accuracy of the government's designations. Such an inquiry would align with a 2012 recommendation from the Government Accountability Office (GAO) to conduct routine assessments that "could help decision makers and Congress determine if the watchlist is achieving its intended outcomes and help inform[] future efforts."[60]

Doing so will be no easy task. Determining with confidence whether someone poses a terrorism risk is close to impossible because "behavioral indicators cannot reliably be used to predict whether an individual will carry out an act of terrorism."[61] Even an individual who may have the "propensity to commit a violent act is still quite likely never to do so."[62] Moreover, because terrorist acts are so infrequent, even a near-perfect tool would misidentify an astounding number of innocent people as would-be terrorists.[63] The reasonable suspicion standard for watch list nominations compounds this situation, as it requires only that a nominator (or reviewer) thinks the candidate "*might* meet the criteria, even if the nominators think they *probably do not*."[64]

Whether for those reasons or others, as a former CIA agent and expert on terrorism has noted, the government has never tested the validity of the various indicators that suffice to place someone on the No Fly List — or, by extension, the TSDB.[65] The Privacy and Civil Liberties Oversight Board (PCLOB) — an independent agency within the executive branch charged with conducting oversight and advising the president — is currently reviewing the TSDB, including the standards for inclusion and procedures to nominate and remove individuals from the list.[66] The PCLOB has not revealed, however, whether its review will include an assessment of watch list efficacy and accuracy.

Inadequate Redress Procedures

No real avenue exists to contest placement on a watch list. U.S. citizens and lawful permanent residents can submit a complaint about travel-related harms — but not about the myriad non-travel-related impacts of being placed on a watch list — through DHS's Traveler Redress Inquiry Program (TRIP).[67] Only Americans on the No Fly List are eligible to receive information about their status. Even then, the program's scope and utility are limited.

When a traveler submits an inquiry through TRIP, TSA and the TSC review the complaint and examine the relevant records. If the traveler is not on the No Fly List, the government provides only a form letter that neither confirms nor denies their status on any other watch list, including the TSDB.[68] Complainants are notified if they are on the No Fly List, but those notifications generally include little explanatory information. Travelers can request an unclassified summary of evidence that landed them on the list, but the government can invoke national security or law enforcement interests to block access to that evidence. When a complainant does receive a response about the basis for inclusion on the list, the information may be almost meaningless. One American Civil Liberties Union (ACLU) client was told only that he was barred from boarding because "he traveled to a particular country in a particular year."[69]

Although the TRIP process can result in removal from the No Fly List or TSDB, no mechanism exists to formally appeal placement on the No Fly List. The head of TSA makes the ultimate determination on TRIP complaints, guided by recommendations from the TSC.[70] Affected travelers may provide additional information to the TSC, but with little explanation as to why they were listed in the first place, they cannot be certain what information might be relevant or persuasive. Travelers dissatisfied with DHS's and the TSC's internal processes have no recourse other than lengthy and expensive legal battles, leaving affected U.S. citizens and lawful permanent residents in a legal limbo that undermines their constitutional rights to travel and due process.[71] And, as Ashraf Maniar experienced, even complainants who do successfully challenge their placement on the No Fly List may remain on the TSDB and other watch lists.

Pattern-Based Profiling

DHS also targets people who are not on any watch list, using opaque programs that, like the watch lists themselves, have effectively been exempted from efforts to systematically assess their effects and their efficacy. Drawing on law enforcement data, classified intelligence, and "patterns of suspicious activity," CBP and TSA attempt to identify patterns of behavior or characteristics ostensibly associated with a range of criminal offenses, from importation of banned agricultural items to human trafficking to terrorism.[72] All travelers, including U.S. citizens and lawful permanent residents, are compared against the resulting rules to gauge whether they pose an elevated risk of committing such offenses. Passengers identified as matching a rule are subjected to increased scrutiny, whether by analysts who conduct additional vetting in databases or by agents who scrutinize travelers and their belongings before they board a plane or upon arrival at a U.S. port of entry.[73]

CBP performs predictive threat modeling using historical data as well.[74] The technical jargon in DHS's public disclosures does not reveal how this process works.[75] In the absence of additional information, it is impossible to know whether these systems have contributed to the rarity of terrorist attacks in the United States since September 11.

Powerful Data Collection and Analysis

At the heart of this risk assessment regime sits the Automated Targeting System (ATS), a massive CBP-owned data repository and analysis tool. ATS was authorized in the years after 9/11 as a means of screening cargo.[76] DHS soon expanded it to include passenger screening,[77] a move that drew a rebuke from the chair of the House Homeland Security Committee.[78] The congressional appropriations committees eventually supported this expansion of the system,[79] but despite the higher stakes of using data-mining tools to target people, DHS has never disclosed its legal justification for doing so.[80]

ATS ingests information pulled from dozens of government databases and other sources, including a DHS database for sharing border information,[81] airline records,[82] searches of electronic devices at the border,[83] department of motor vehicle (DMV) registrations,[84] and criminal records from the FBI, along with social media data and other information compiled and sold by commercial aggregators.[85] DHS components compare information available about travelers through ATS against watch lists, criminal records, warrants, and "patterns of suspicious activity."[86]

For example, if CBP obtains intelligence, either directly or through a partner agency, indicating that people who have spent time in a particular region present an elevated risk of committing a terrorist act, it could likely create a rule within ATS that flags pieces of data in its stockpile indicating travel in that region, such as departure and arrival records, information from nonimmigrant visa applications, and information uncovered through prior interrogations.[87] When travelers match this rule, an analyst can consult additional records and instruct officers at ports of entry to inspect or question the individuals. Publicly available materials provide only superficial information about how this process works.

Lack of Evaluation

As with the watch lists, DHS has never conducted a public empirical evaluation of ATS's effectiveness or of the relative value of the risk assessments it enables, nor has the department weighed its benefits against risks to Americans' privacy. This remains the case despite multiple GAO reviews urging the department to establish measures to evaluate the performance of its screening programs.[88]

DHS does share anecdotes about ATS's execution in the data-mining reports that it sends annually to Congress. These reports, which have been required by statute since 2007, describe the department's analysis of government data to unearth patterns ostensibly related to criminal or terrorist activity.[89] ATS has been included in every data-mining report since their inception. A Brennan Center review of every published report revealed few meaningful successes.

In its 14 published reports,[90] presumably covering tens of millions of screening events, DHS described 29 cases in which ATS assisted CBP officers in identifying people for increased scrutiny, leading to their apprehension or denial of entry into the country.[91] Of these, only nine involved further CBP inspection of a traveler based expressly on ATS's assessment of risk. In one instance, ATS prompted the National Targeting Center to vet a traveler whom analysts categorized as "a possible affiliate of a person listed in the TSDB."[92] The remainder of the risk-related case studies feature situations in which ATS helped identify people who were involved in drug trafficking and traveled with doctored documents. None of the case studies showcase ATS's predictive modeling capabilities.

These anecdotes may not represent the full universe of ATS's uses. Regardless, their haphazard nature highlights the absence of any comprehensive data with which to evaluate the system's usefulness. DHS also does not disclose how many people flagged as high-risk did not go on to commit a criminal or terrorist act, or how many people were not flagged but nevertheless went on to commit a crime for which ATS purports to screen. Nor is there any information about the quality and accuracy of the data in ATS, although DHS's inspector general recently urged the department to shore up a far-reaching TSA program, Quiet Skies, that relies heavily on ATS, including by instituting performance measures and ensuring the reliability of Quiet Skies data (which would include data from ATS).[93] In short, DHS has not publicly shown that ATS's value justifies its scale and cost. And one former DHS official's observation that "rule-sets in the passenger environment outperform random inspection, but not always by much" underscores the fact that effectiveness cannot be taken for granted.[94]

Tactical Terrorism Response Teams

>> Tactical Terrorism Response Teams (TTRTs) are composed of CBP officers and Border Patrol agents trained to conduct counterterrorism investigations. They work closely with and are overseen by the NTC.[95] Created in 2015, TTRTs are stationed at ports of entry throughout the country to examine travelers who are watch-listed or "suspected of having a nexus to terrorist activity," though their mission has expanded to include counterintelligence, transnational organized crime, and biological threats.[96] Between 2017 and 2019, TTRTs detained and interrogated more than 600,000 travelers — including 180,000 U.S. citizens — and even denied some Americans entry into the country.[97]

TTRTs were created in part to leverage officers' "instincts" to identify people who are not on the watch lists but who may nevertheless pose threats — an open invitation for pretextual targeting and discriminatory profiling.[98] TTRT officers may carry out an "intensive secondary inspection, document review, interview/questioning, and examination" to uncover information from and about people they deem suspicious, and funnel their findings back to the NTC.[99] This information then flows into ATS.[100]

In several well-documented cases, TTRT officers have used their authority to launch fishing expeditions targeting Americans' First Amendment–protected activity. In February 2017, the NTC directed TTRT officers to interrogate Aaron Gach, an activist sculptor and art professor, when he returned to San Francisco from an art show in Belgium.[101] Gach is the founder of the Center for Tactical Magic, a nonprofit arts collective that creates provocative exhibits critiquing U.S. policing and surveillance policies. Officers questioned Gach about his art practice, the Belgian exhibition, and his contacts abroad and prohibited him from leaving until he unlocked his cell phone. The following year, TTRT officers subjected Andreas Gal to a similar interrogation, also in San Francisco. Gal, an Apple technologist and the former chief technology officer of Mozilla, had been outspoken on social media about his support for online privacy and his opposition to the Trump administration's immigration policies. A complaint letter from the ACLU to DHS alleges that Gal was "questioned about his travel plans, his work at Apple, his employment history, and his electronic devices," including detailed questions about his activities at Mozilla. He asked to consult with a lawyer before providing the passwords to his employer-provided electronic devices, which contained confidential and proprietary information. In response, TTRT officers threatened him with criminal prosecution and confiscated his Global Entry membership card, warning that he would be removed from the program.[102]

In April 2022, DHS's Office for Civil Rights and Civil Liberties initiated an investigation after it received at least 11 complaints that TTRT officers had questioned travelers about their religious beliefs and practices, used First Amendment–protected information as the basis for denying them entry into the United States, and unjustifiably seized or searched their electronic devices, among other allegations. Eight of the complaints involved U.S. citizens, and most of the complainants were Muslim or of Middle Eastern descent.[103] The results of CRCL's investigation have not yet been published.

Intrusive Inspections and First Amendment Violations

Once a traveler is flagged for scrutiny, CBP officers have wide latitude to conduct a secondary inspection that can produce a wealth of information about First Amendment–protected activity. This includes interrogation notes, documentation of materials in travelers' luggage, or data obtained through electronic device searches.[104] Individuals who have received their ATS files through Privacy Act requests have even found officers' notes about books they carried and conferences they attended.[105] Searches of electronic devices are particularly concerning given the volume and personal nature of information stored on laptops and cell phones. The DHS inspector general has twice criticized CBP for failing to comply with its own policy on device searches. The inspector general's reports from 2018 and 2021 revealed that agents had neglected to document their searches and failed to disable devices' network connections to prevent access to information stored remotely. These oversights could have allowed CBP agents to access emails, social media data, and other data that travelers had taken care to transfer from their device's local storage to cloud or other remote storage, all of which the policy prohibits border officers from accessing during routine searches.[106]

The NTC, which produces CBP's intelligence-based rules, has itself abused its authority in ways that undermine First Amendment protections. One officer at a secretive entity within the NTC, the Counter Network Division, exploited his access to TECS, ATS, and other government databases to investigate journalists, government officials, lawmakers, and congressional staff as part of a leak investigation.[107] A follow-up investigation found that the division was monitoring Americans to uncover information about protests marking the one-year anniversary of the January 6 insurrection and opposing President Joe Biden's inauguration — matters that extend far beyond the bounds of CBP's border security mandate.[108]

TECS Database

>> DHS agents rely on the TECS database to collect data about travelers and screen people at ports of entry.[109] TECS, which CBP maintains, contains individualized records that are created before travelers arrive at a port of entry and during transit, as well as when travelers are referred from primary to secondary inspection. A secondary inspection may be triggered by a match against a watch list or a rule or because an event occurs to flag the traveler as warranting additional scrutiny.[110] TECS allows its more than 85,000 users to screen people against a huge repository of data that includes travel and border crossing records, the TSDB, and civil and criminal records from the FBI's centralized records database.[111] Law enforcement agents also use TECS to place "lookouts," which alert border officers that flagged individuals have arrived at a port of entry so they can be stopped and inspected.[112]

TECS has been abused to target travelers for political reasons. During the Trump administration, CBP used TECS to place lookouts on U.S. citizens — including journalists, activists, humanitarian workers, and even a pastor — in retaliation for their support of a migrant caravan approaching the southern border. These lookouts led to lengthy secondary inspections that discouraged their subjects' peaceful, constitutionally protected work.[113] Pastor Kaji Douša, whom CBP targeted for ministering to migrants, sued DHS after her name was put in a TECS lookout and a CBP officer requested that Mexico deport her on grounds that he later admitted were invented. In 2023, a federal district court ruled that DHS's actions amounted to retaliation in violation of Douša's First Amendment rights.[114]

TECS was also used during the Obama administration to target David House, a computer programmer who cofounded the legal defense fund for U.S. Army whistleblower Chelsea Manning. On his return from a trip to Mexico in 2010, border agents stopped House and interrogated him about his political activities and beliefs, seizing his electronic devices, including his laptop, and copying and analyzing their data.[115] Documents revealed after House filed suit showed that agents from Immigration and Customs Enforcement (ICE), another DHS agency, had placed a TECS lookout on his name. ICE ultimately concluded that none of the data indicated criminal activity. Nevertheless, TECS's long retention period permits storage of this information for up to 75 years, a policy that compounds First Amendment harms by enabling border officers to repeatedly view sensitive details.[116]

Recommendations

In the two decades since its founding, DHS has institutionalized a vast architecture to collect and analyze data about hundreds of millions of Americans and non-Americans alike. Any discussion about these systems must confront the question of whether resources should continue to flow to government programs that are entirely unproven — indeed, programs designed in part to predict events so rare that they are likely unsusceptible to predictive analysis. These recommendations focus on crucial steps that would begin to ameliorate the problems identified in this report and elicit the information necessary to determine the programs' future viability.

>> Disclose additional information about risk-related programs.

There is a woeful lack of publicly available information about the government's risk analysis and prevention systems — both the TSDB and its subsidiary lists and DHS's pattern-based programs. The department should disclose (and where necessary declassify) consequential materials, prioritizing the following:

- reports, policies, and similar documents that describe, explain, or govern the relevant systems and how they operate;
- documentation that addresses DHS's legal justification for its expansion of ATS; and
- agreements with private companies relating to purchases of or subscriptions to data or analytic tools.[117]

Similar efforts by the FBI and the Office of the Director of National Intelligence with respect to the TSDB and its ancillary watch lists should accompany these disclosures. For one, the TSC or the NCTC should publicly clarify the date of the current watch-listing guidance and disclose the legal standard used to designate people as known or suspected terrorists and place them on the TSDB, the No Fly List, or the Selectee List. In addition, the FBI should disclose the identities of nonfederal recipients of the TSDB.

>> Evaluate risk assessment programs and watch lists.

An independent, rigorous investigation and evaluation of the government's risk assessment regime, from the FBI's watch lists (the TSDB, the No Fly List, and the Selectee List) to DHS's rules-based and algorithm-driven screening programs, is long overdue.[118] The PCLOB is already examining the TSDB, and its mission and legal authorities position it well to expand the scope of that inquiry. Alternatively, Congress could create a special commission or a time-limited special inspector general to undertake this task.[119]

This investigative body must have the authority and clearance to review classified intelligence and access to all existing reviews of and complaints about the programs, whether previously published or not. It should also have staff expertise in empirical methodologies for program evaluation and in privacy, civil rights, and civil liberties concerns, and it should provide a means to solicit and consider public input. Existing work in the field, including frameworks for managing risk in artificial intelligence (AI) systems and recent executive branch guidance on equity in AI-driven programs, should inform its efforts.[120] Investigators should prioritize the following:

- examining ATS, including the processes within TSA and CBP to propose and oversee risk-based rules incorporated into ATS, how ATS matches individuals against risk-based rules, and how it makes pattern-based predictions;
- establishing evaluation metrics for the TSDB and its downstream watch lists, as well as for the department's risk-based rules and predictive analytics programs, including defining what constitutes success for each program, articulating and instituting mechanisms to measure success, assessing bias, identifying any additional data that should be collected to assist in measuring the programs' accuracy, and implementing an empirical evaluation protocol; and
- assessing whether adequate protections are in place to prevent misuse of TECS to target activity related to religious, political, or other expression, and whether TECS's scope and retention period could be narrowed without compromising DHS's counterterrorism and public safety missions.

At the close of its work, the reviewing entity should inform Congress, the FBI, and DHS of its findings and issue public reports detailing its conclusions. Along with their findings, the reports should articulate the investigative methodology and any recommendations regarding continued evaluation and oversight of each of the abovementioned priorities. The recommendations should include concrete steps for the agencies and relevant components to evaluate both data quality and program efficacy.

The reports should be drafted with a presumption in favor of public disclosure; and any classified annexes should be summarized in a public format. In addition, Congress should hold regular hearings with both public and (where necessary) classified components to assess the agencies' compliance with the recommended measures and to facilitate the implementation of lessons learned, including steps to narrow the programs or discontinue aspects of them.

>> Bolster the redress process for those on the TSDB and the No Fly List.

DHS should provide U.S. citizens and lawful permanent residents with robust mechanisms to elicit information about and challenge their placement on the watch lists without having to pursue expensive and time-consuming litigation.[121] For the No Fly List, DHS should adopt an approach similar to the Canadian model and affirmatively inform individuals of their status when they are conclusively determined to be ineligible for boarding, rather than requiring them to file a complaint. In addition, affected travelers should receive information that is sufficient to allow them to challenge their presence on a watch list, whether directly or through a bar of attorneys cleared to view relevant classified information.

Outside the No Fly List context, DHS has asserted that notifying complainants of their TSDB status is too risky because terrorist groups could use the complaint process to assess which of their members are *not* on the watch list. Absent any empirical evaluation of the lists and their effectiveness, the credibility or significance of this concern remains a matter of conjecture. The government has justified other programs on the basis of acute national security concerns that ultimately proved to be unsupported by evidence.[122] Additional fact-finding is thus needed to substantiate the department's claim. Regardless, U.S. citizens and lawful permanent residents should have an avenue to challenge their placement on the TSDB.

>> Evaluate the integrity of the TSDB nomination process.

As DHS's watch-listing lead, I&A is responsible for offering guidance to DHS components on the TSDB nominations process to ensure that nominations are supported by sufficient information and meet the relevant standards. That process frequently falls short, owing in part to I&A's inability to compel the components to comply with its directives. The involvement of multiple agencies complicates the matter.

In consultation with DHS and the FBI, the Office of the Director of National Intelligence (under which the National Counterterrorism Center operates) should audit a representative sample of the nominations accepted to the TSDB, assessing the quality of the underlying derogatory data alongside any potential countervailing data. The office should issue a public report on the audit's findings and recommendations. It should then make recommendations regarding the nominations process that I&A could help implement, focusing on substantially reducing the size of the watch lists considering the issues articulated in this report. The secretary of homeland security should direct DHS components to follow I&A's guidance.

Conclusion

DHS's interlocking data holdings and risk assessment programs have far too often been deployed in discriminatory ways that stretch beyond their original purposes and violate Americans' constitutional rights and civil liberties. DHS and its partners in these efforts have failed to institute any systematic mechanisms to test their efficacy, nor have they defined success or articulated what costs are justified. This report's recommendations, if adopted, would better align DHS's risk assessment regime with key American values and priorities, including protecting constitutional rights, ensuring that government resources are expended for programs that actually work, and safeguarding national security.

Endnotes

[1] DHS's practices also harm those who are not U.S. citizens or lawful permanent residents, but this report's primary focus is how they affect Americans.

[2] See, e.g., National Immigration Law Center, *Homeland Advanced Recognition Technology (HART): DHS Is Building a Massive Database of Personal Information*, November 16, 2021, https://www.nilc.org/wp-content/uploads/2021/12/HART-factsheet-2021-11-10.pdf; and Mizue Aizeki and Paromita Shah, *HART Attack: How DHS's Massive Biometrics Database Will Supercharge Surveillance and Threaten Rights*, Immigrant Defense Project, Just Futures Law, and Mijente, May 2022, https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/635c0b2b52d90a16d78ba2dd/1666976559030/HART+Attack.pdf.

[3] "'Screening' is an automated query of . . . data points," such as personally identifiable information, against government databases to "identify possible matches to derogatory information. 'Vetting' is a manual review of potential derogatory information identified in the screening." Office of Inspector General (hereinafter OIG), *ICE and CBP Should Improve Visa Security Program Screening and Vetting Operations*, Department of Homeland Security (hereinafter DHS), September 16, 2022, 2n1, https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-70-Sep22.pdf.

[4] DHS conducts other types of individualized checks as well. As a former DHS official explained, "DHS can determine whether the address listed on a form [such as a customs declaration] is also listed by a known or suspected malefactor, or whether the credit card used to purchase a plane ticket was also used to purchase the ticket of a different individual found to be a 'bad guy.'" Chappell Lawson, "The Trusted and the Targeted: Segmenting Flows by Risk," in *Beyond 9/11: Homeland Security for the Twenty-First Century*, ed. Chappell Lawson, Alan Bersin, and Juliette N. Kayyem (Cambridge, MA: MIT Press, 2020), 113.

[5] The TSDB contains only identifying information about the people on the list, not the underlying substantive justifications for placing them on the list; this enables broad sharing of the list with agencies and other third parties not authorized to view classified information. In 2022, the government announced that it changed the name of the TSDB to the "Terrorist Screening Dataset," but many sources continue to refer to it as the TSDB. Declaration of Jason Herring at ¶ 5, Moharam v. FBI, No. 21CV02607 (D.D.C. January 18, 2022).

[6] Elhady v. Kable, 391 F. Supp. 3d 562, 568 (E.D. Va. 2019), overruled on other grounds by Elhady v. Kable, 993 F.3d 208 (4th Cir. 2021). A version of a watch list that was exposed online in 2021 contained some 1.9 million records. Shoshana Wodinsky, "Secret FBI Watchlist Leaks Online, and Boy Do the Feds Think a Lot of People Are Terrorists," *Gizmodo*, August 17, 2021, https://gizmodo.com/secret-fbi-watchlist-leaks-online-and-boy-do-the-feds-1847500747. It is unclear whether the watch list exposed online in 2021 is complete, whether each of the records it contains corresponds to a unique individual, or how many of the records correspond to Americans.

[7] TSC stood for Terrorist Screening Center until January 2021, when the government renamed it. *Criminal Justice Information Services Division, National Crime Information Center (NCIC) Technical and Operational Update (TOU) 21-3*, FBI, June 11, 2021, § 2.1, https://isp.idaho.gov/bci/wp-content/uploads/sites/3/2021/06/TOU-21-3.pdf.

[8] The guidance is developed by the Watchlisting Advisory Council (an interagency group that includes representatives from DHS, NCTC, the Department of Justice, and other agencies) and is approved by the White House's National Security Council. Declaration of Jason Herring at ¶¶ 6, 9, Jardaneh v. Barr, No. 18CV02415 (D. Md. June 11, 2020) (case originally filed as El Ali v. Sessions). The 2013 version of the guidance was leaked online but was not released publicly. National Counterterrorism Center (hereinafter NCTC), *Watchlisting Guidance*, March 2013, https://www.aclu.org/wp-content/uploads/legal-documents/March%202013%20Watchlist%20Guidance.pdf. The government has represented in court filings that similar (though not identical) guidance was issued in 2015, superseding the 2013 guidance. Declaration of Timothy P. Groh Submitted in Camera, *Ex Parte* in Response to Plaintiffs' Second Motion to Compel at ¶ 23, Elhady v. Kable, No. 16CV000375 (E.D. Va. April 27, 2018). In 2018, the TSC released an overview document that summarizes the watch-listing process — the only such document released publicly by the government. Terrorist Screening Center, *Overview of the U.S. Government's Watchlisting Process and Procedures*, April 27, 2018 (hereinafter TSC, *Watchlisting Process and Procedures*), 3, https://www.aclu.org/sites/default/files/field_document/ex._7_elhady_-_overview_of_watchlisting_system_-_4-27-18_cover.pdf. Updated guidance may also have been issued in 2018. Brief of *Amicus Curiae* Council on American-Islamic Relations (hereinafter CAIR) in Support of Petitioner's Writ of Certiorari at 10n12, Americans for Prosperity Foundation v. Bonta, 141 S. Ct. 2373 (2021), https://www.supremecourt.gov/DocketPDF/19/19-251/169893/20210224161321178_CAIR%20AFP%20Amicus%20File%20Version.pdf (originally argued as Americans for Prosperity Foundation v. Becerra).

[9] TSC, *Watchlisting Process and Procedures*, 3.

[10] Nominations that meet NCTC standards for international terrorism are also entered into the NCTC's Terrorist Identities Datamart Environment (TIDE), the government's highly classified central repository of information about alleged international terrorists.

[11] TSC, *Watchlisting Process and Procedures*, 3 (stating that nominating agencies "provide identities" to the FBI when they have "a nexus to domestic terrorism"); and Jerome Bjelopera, Bart Elias, and Alison Siskin, *The Terrorist Screening Database and Preventing Terrorist Travel*, Congressional Research Service, November 7, 2016, 3, https://sgp.fas.org/crs/terror/R44678.pdf (depicting the FBI as the sole entity nominating "identities of known or suspected domestic terrorists" to the TSC). Domestic terrorism is defined by statute as criminal activities committed "primarily within" U.S. territory that are "dangerous to human life" and "appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping." 18 U.S.C. § 2331(5) (2004).

[12] See Complaint at ¶ 85, Chebli v. Kable, No. 21CV00937 (D.D.C. April 6, 2021), https://www.aclu.org/cases/chebli-v-kable-lawsuit-challenging-placement-no-fly-list?document=chebli-v-kable-complaint#legal-documents (noting that from 2008 to 2017, the TSC rejected just 1.4 percent of the more than 1.1 million TSDB nominations that it received).

[13] A person may be added to the No Fly List if they are reasonably suspected to pose a threat of committing a terrorist act aboard an aircraft or against any U.S. government facility (abroad or within U.S. territory), or if they represent a threat of "engaging in or conducting a violent act of terrorism" and are "operationally capable of doing so." TSC, *Watchlisting Process and Procedures*, 4; and Brief of *Amicus Curiae* Jeffrey Khan in Support of Respondents at 12–13, Tanzin v. Tanvir, 141 S. Ct. 486 (2020), https://scholar.smu.edu/cgi/viewcontent.cgi?article=1650&context=law_faculty (noting that reasonable suspicion is also the standard for inclusion on the No Fly List). As of the 2013 watch-listing guidance, an individual could be included on the Selectee List if they fell below the No Fly List's standard for inclusion but were a member of a terrorist organization and were associated with "terrorist activity," though the guidelines do not define the nature of that association. NCTC, *Watchlisting*

Guidance, 55. See also 8 U.S.C. § 1182(a)(3)(B)(iii) (2014) (defining terrorist activity). The government has stated that "the criteria for inclusion on the Selectee List are not public," which may indicate that the criteria have changed since the leaked 2013 guidance or simply that the guidance is not technically considered public since the NCTC has not voluntarily released it. TSC, *Watchlisting Process and Procedures*, 4.

14 TSC, *Watchlisting Process and Procedures*, 5; Bjelopera, Elias, and Siskin, *Terrorist Screening Database and Preventing Terrorist Travel*, 7–8; Bart Elias, "Aviation Security Measures and Domestic Terrorism Threats," Congressional Research Service, January 15, 2021, 1, https://crsreports.congress.gov/product/pdf/IF/IF11731/2; and Jonathan Cantor, *Privacy Impact Assessment Update for Secure Flight*, DHS Privacy Office, July 12, 2017, 1–2, https://www.dhs.gov/sites/default/files/publications/pia_tsa_secureflight_18%28h%29_july2017.pdf.

15 *Elhady*, 993 F.3d at 214; TSC, *Watchlisting Process and Procedures*, 5; and *Supporting a Fact-Based Approach to Preventing Terrorist Travel to the United States, Joint Hearing Before the Subcomm. on Intelligence and Counterterrorism and the Subcomm. on Border Security, Facilitation, and Operations of the H. Comm. on Homeland Security*, 116th Cong. (2019) (testimony of Donald Conroy, NTC director), https://www.govinfo.gov/content/pkg/CHRG-116hhrg36398/html/CHRG-116hhrg36398.htm.

16 International Refugee Assistance Project and CAIR New York, "Know Your Rights at the Airport," accessed September 12, 2023, https://refugeerights.org/wp-content/uploads/2017/12/IRAP_KYR_Flyer.pdf.

17 Kevin McAleenan, CBP Directive No. 3340-049A: Border Search of Electronic Devices, U.S. Customs and Border Protection (hereinafter CBP), January 4, 2018, 5, https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

18 See Department of Justice (hereinafter DOJ) Office of Privacy and Civil Liberties, notice of proposal to amend system of records for the Terrorist Screening Records System (Justice/FBI-019), 72 Fed. Reg. 47073, 47078 (August 22, 2007), https://www.federalregister.gov/documents/2007/08/22/E7-16487/privacy-act-of-1974-system-of-records (permitting disclosure of the TSDB to "any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, multinational or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities"); *Elhady*, 391 F. Supp. 3d at 570 ("TSDB data is also shared with more than sixty foreign governments with which the TSC has entered into foreign partner arrangements, which, subject to their domestic laws and the restrictions in the agreements, use the information for terrorist screening purposes."); *Elhady*, 391 F. Supp. 3d at 568 (noting that foreign governments can nominate people to the TSDB); and Murtaza Hussain, "Local Cops Harassed and Threatened U.S. Veteran Because of Terror Watchlist, Lawsuit Says," *Intercept*, January 26, 2023, https://theintercept.com/2023/01/26/terror-watchlist-police-harassment.

19 White House, *National Strategy to Combat Terrorist Travel of the United States of America*, December 2018, 14, https://www.brennancenter.org/sites/default/files/2023-10/Natl%20Strategy%20for%20Combatting%20T.%20Travel.pdf. The 2013 guidance also permitted a single, uncorroborated source to suffice and did not require "concrete facts" when nominating people to the watch lists. Whether the current guidance includes the same standard is not known. NCTC, *Watchlisting Guidance*, 34. See also Shirin Sinnar, "Rule of Law Tropes in National Security," *Harvard Law Review* 129, no. 6 (April 2016): 1597, https://harvardlawreview.org/print/vol-129/rule-of-law-tropes-in-national-security.

20 Mohamed v. Holder, 995 F. Supp. 2d 520, 532 (E.D. Va. 2014).

21 See Anya Bernstein, "The Hidden Costs of Terrorist Watch Lists," *Buffalo Law Review* 61, no. 3 (May 2013): 487, https://digitalcommons.law.buffalo.edu/journal_articles/63.

22 Under its 2013 guidance, "NCTC will rely on the designation of 'known terrorist' provided by the nominator as presumptively valid" unless that designation is contradicted by "specific and credible information" to the contrary. NCTC, *Watchlisting Guidance*, 21.

23 *Chebli*, complaint at ¶ 85. See also *Elhady* 993 F.3d at 214.

24 TSC, *Watchlisting Process and Procedures*, 6.

25 *Elhady*, 391 F. Supp. 3d at 581–82.

26 NCTC, *Watchlisting Guidance*, 21 (identifying I&A as the lead for the department). See also OIG, *DHS' Watchlisting Cell's Efforts to Coordinate Departmental Nominations (Redacted)*, DHS, July 2013, 48–49, https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/2013/OIG_13-105_Jul13.pdf (describing I&A's duties as including "(1) establishing, managing, and overseeing a unified watchlisting capability for the Department; (2) issuing DHS-wide terrorist watchlisting nomination policies, procedures, guidelines, and standards consistent with Federal watchlisting guidance; and (3) representing the Secretary in all interagency forums relating to terrorist watch listing nominations").

27 See Declaration of Marc Sageman in Opposition to Defendants' Cross-motion for Summary Judgment at 19–20, Latif v. Lynch, No. 10CV00750 (D. Or. August 7, 2015), https://www.aclu.org/sites/default/files/field_document/268._declaration_of_marc_sageman_8.7.15.pdf (describing the various incentive systems that foster false positives and observing that "FBI special agents are promoted and rewarded — even with monetary bonuses — based on providing derogatory information on U.S. persons, while admission of error or new information that exonerates someone from suspicion tends not to be rewarded"); and Bernstein, "Hidden Costs of Terrorist Watch Lists," 473 ("A large list of terror suspects suggests that terrorist activities are likely. That, in turn, suggests that more resources should be devoted to agencies that deal with terrorism.").

28 Timothy Goyer, *Improvements, Questions, and Limits for the Future of Watchlisting*, Center for Strategic and International Studies, April 2020, 3, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200421_Goyer_FutureWatchlisting_WEB%20FINAL.pdf. See also *Latif*, Sageman declaration at 19 (noting that the intelligence community's goal of eliminating the threat of terrorism is an impossible one that "results in a system of incentives that encourages the generation of false positives").

29 OIG, *Follow-Up Audit of the Terrorist Screening Center*, DOJ, September 2007, iii, https://oig.justice.gov/reports/FBI/a0741/final.pdf.

30 OIG, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, DOJ, May 2009, iv, vi, https://oig.justice.gov/reports/FBI/a0925/final.pdf.

31 OIG, *Audit of the Federal Bureau of Investigation's Management of Terrorist Watchlist Nominations*, DOJ, March 2014, 15, 19, 22, 24, https://oig.justice.gov/reports/2014/a1416.pdf. See also Shirin Sinnar, "Terrorist Watchlists and the Myth of Individual Suspicion," *Just Security* (blog), May 1, 2014, https://www.justsecurity.org/10068/guest-post-terrorist-watchlists-myth-individual-suspicion.

32 Mikael Thalen and David Covucci, "Exclusive: U.S. Airline Accidentally Exposes 'No Fly List' on Unsecured Server," *Daily Dot*, last modified June 2, 2023, https://www.dailydot.com/debug/no-fly-list-us-tsa-unprotected-server-commuteair; and Edward Hasbrouck, "The #NoFly List Is a #MuslimBan List," *Papers, Please!* (blog), January 20, 2023, https://papersplease.org/wp/2023/01/20/the-nofly-list-is-a-muslimban-list. According to an analysis of the leaked watch list from 2019, the No Fly List contained 3 four-year-olds and 25 centenarians. Hasbrouck, "#NoFly List Is a #MuslimBan List."

33 Whether the list exposed online represents the entirety of the TSDB or just a portion of it remains uncertain. See Volodymyr Diachenko, "America's Secret Terrorist Watchlist Exposed on the Web

Without a Password: Report," LinkedIn, August 16, 2021, https://www.linkedin.com/pulse/americas-secret-terrorist-watchlist-exposed-web-report-diachenko.

34 David Park, "The Watchlist: Improving the Transparency, Accuracy, Efficiency, and Accountability of the Terrorist Screening Database," master's thesis, Naval Postgraduate School, December 2018, 70–71, https://apps.dtic.mil/sti/pdfs/AD1069685.pdf.

35 See Civil Rights Litigation Clearinghouse, "Case: Ibrahim v. Department of Homeland Security," University of Michigan Law School, accessed September 12, 2023, https://www.clearinghouse.net/detail.php?id=13632.

36 Murtaza Hussain, "One Man's No-Fly List Nightmare," *Intercept*, May 30, 2021, https://theintercept.com/2021/05/30/no-fly-list-terrorism-watchlist.

37 Intercept, "One Man's No-Fly List Nightmare," YouTube, May 30, 2021, at 7:40, https://www.youtube.com/watch?v=-xnpau6LXhU.

38 See Second Amended Complaint at 13, Maniar v. Wolf, No. 19CV03826 (D.D.C. September 9, 2020). In a recent lawsuit on behalf of Muslim American citizens, lawful permanent residents, and asylees who know or believe they are on the TSDB, CAIR alleges that government agencies consider being a "relative, friend, colleague, or fellow community member" of a watch-listed individual to be "derogatory information" that could support a nomination to the watch list. The lawsuit also alleges that CBP and TSA programs that screen travelers "often flag listees' travel companions as themselves being potential terrorists," leading to enhanced scrutiny. Complaint at ¶¶ 307, 362, Khairullah v. Garland, No. 23CV30095 (D. Mass. September 18, 2023), https://www.cair.com/wp-content/uploads/2023/09/D.-Mass.-23-cv-30095-dckt-000001_000-filed-2023-09-18.pdf. One plaintiff reported that FBI agents asked to search his infant, and another noted that he will no longer cross the U.S.-Canadian border with his children "for fear of subjecting them to detention, harassment, invasive searches, and other humiliating ordeals as a result of his placement on the watchlist." *Khairullah*, complaint at ¶¶ 624, 979.

39 CAIR's recent lawsuit asserts that "Muslim communities are subjected to rapidly-unfolding network effects once one member is watchlisted," with the government classifying "nearly every member of an extended family or community mosque as a suspected terrorist." *Khairullah*, complaint at ¶ 362.

40 TSC, *Watchlisting Process and Procedures*, 4. See also Harsha Panduranga and Faiza Patel, *Stronger Rules Against Bias: A Proposal for a New DHS Nondiscrimination Policy*, Brennan Center for Justice, September 9, 2022, 2, https://www.brennancenter.org/our-work/policy-solutions/stronger-rules-against-bias; and *Khairullah*, complaint at ¶ 9 (alleging that the government considers "origin from Muslim-majority countries, travel to Muslim-majority countries, attending mosques and Islamic events, *zakat* donations to Muslim charities, the wearing of typical Muslim dress, Muslim-sounding names, the frequency of Muslim prayer," and other similar factors "to be suspicious, and routinely nominate[s] Muslims to the watchlist on the basis of those characteristics and activities").

41 CAIR, *Twenty Years Too Many: A Call to Stop the FBI's Secret Watchlist*, June 2023, 13, https://www.cair.com/wp-content/uploads/2023/06/watchlistreport-1.pdf.

42 Hasbrouck, "#NoFly List Is a #MuslimBan List."

43 Aamer Madhani, "Muslim Mayor Blocked from White House Eid Celebration," Associated Press, May 1, 2023, https://apnews.com/article/new-jersey-mayor-white-house-eid-8e67495af3cd982a6560d1121a29e8ba. In September 2023, CAIR filed a lawsuit on behalf of Mayor Khairullah and eleven other plaintiffs challenging the government's watch listing regime. *Khairullah*, complaint; and Daniel Han, "Muslim New Jersey Mayor Denied Entry to White House Plans Lawsuit Against 'Watchlist'," *Politico*, September 15, 2023, https://www.politico.com/news/2023/09/15/muslim-new-jersey-mayor-denied-entry-to-white-house-plans-lawsuit-00116358. According to the complaint, Khairullah believes that his name was removed from the watch list by May 2023 but is still negatively affected by his prior inclusion on the TSDB. *Khairullah*, complaint at ¶ 461.

44 Complaint at ¶¶ 8, 47–49, 58–59, 90–93, Kariye v. Mayorkas, No. 22CV01916 (C.D. Cal. March 24, 2022). See also Deena Zaru, "Muslim American Speaks Out on Suing DHS, Border Officials over 'Intrusive' Religious Questioning," ABC News, March 28, 2022, https://abcnews.go.com/US/muslim-american-speaks-suing-dhs-border-officials-intrusive/story?id=83649104; and CAIR, *Twenty Years Too Many*, 6 (documenting clients' stories about being questioned at the border about their Islamic faith and practice, including a female client being told to remove her hijab if she wished to travel without delays). Kariye's case was dismissed in July 2023; in September 2023, the plaintiffs appealed the court's dismissal to the Ninth Circuit Court of Appeals. Order Granting Defendants' Motion to Dismiss, Kariye, No. 22CV01916 (C.D. Cal. July 19, 2023); and Plaintiffs' Notice of Appeal, Kariye, No. 22CV01916 (C.D. Cal. September 18, 2023).

45 *Khairullah*, complaint at ¶ 540.

46 *Khairullah*, complaint at ¶¶ 622–23. Tawhidullah Amini, another plaintiff in the lawsuit, was detained when he returned to Chicago from visiting his family in Afghanistan in May 2018; according to the complaint, CBP officers interrogated him about "what he thought about a particular medieval Muslim scholar, [the] school of thought he adheres to, what mosque he attends, whether he prays regularly, and if he follows the Salafi sect of Islam." *Khairullah*, complaint at ¶¶ 814, 818.

47 Margo Schlanger (officer, Office for Civil Rights and Civil Liberties), DHS, letter to Laura Murphy (director, Washington Legislative Office, ACLU), Farhana Khera (president and executive director, Muslim Advocates), and Hina Shamsi (director, National Security Project, ACLU), May 3, 2011, 1, https://www.aclu.org/sites/default/files/field_document/2011_05_03_DHS_Letter_re_Border_Questioning.pdf.

48 Schlanger, letter to Murphy, Khera, and Shamsi; Tamara Kessler (acting officer, CRCL), letter to Laura Murphy (director, Washington Legislative Office, ACLU), Farhana Khera (president and executive director, Muslim Advocates), and Hina Shamsi (director, National Security Project, ACLU), July 12, 2012, 1, https://www.aclu.org/sites/default/files/field_document/2012.07.12_homeland_security_response.pdf; Cherri v. Mueller, No. 12CV11656 (E.D. Mich. April 13, 2012), complaint (the case remains ongoing as of this report's publication); and Nusrat Choudhry (staff attorney, ACLU), Glenn Katon (legal director, Muslim Advocates), and Mike German (senior policy counsel, Washington Legislative Office, ACLU), letter to Charles K. Edwards (acting inspector general, DHS), April 15, 2012, https://www.aclu.org/wp-content/uploads/document/dhs_ig_letter__appendix__exhibits_04152013.pdf (criticizing CRCL for suspending the investigation, purportedly in response to a lawsuit, *Cherri v. Mueller*, that did not represent ACLU complainants).

49 See Dena Kozanas, *Privacy Impact Assessment for the Watchlist Service*, DHS Privacy Office, July 10, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall027d-watchlistservice-july2020.pdf; Erin M. Prest, *Privacy Impact Assessment for the National Crime Information Center*, DOJ Office of Privacy and Civil Liberties, November 7, 2022, 6, https://www.fbi.gov/file-repository/pia-ncic-020723.pdf/view; Hussain, "Local Cops Harassed and Threatened U.S. Veteran Because of Terror Watchlist"; and Ann Davis, "Use of Data Collection Systems Is Up Sharply Following 9/11," *Wall Street Journal*, May 22, 2003, https://www.wsj.com/articles/SB105355527183611100 (documenting the experience of a Denver gun rights group member who was stopped after a minor car accident and discovered he was listed as "a member of a terrorist organization," even though the underlying files documenting constitutionally protected activity were supposed to have been purged) (cited in Bernstein, "Hidden Costs of Terrorist Watch Lists," 467). See also Park, "Watchlist," 39 (describing the TSDB's intelligence-gathering function). Information-sharing hubs called fusion centers, whose issues we have chronicled in a previous report, also have access to watch list data through their state and local law enforcement partners. See Office of Justice Programs, *Fusion Center Technology Guide: DHS/DOJ Fusion Process Technical Assistance Program and Services*, DOJ, April 2009, 14, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_technology_guide.pdf; and Michael German, Rachel Levinson-Waldman, and Kaylana Mueller-Hsia, *Ending Fusion Center Abuses: A Roadmap for Robust Federal Oversight*, Brennan Center for Justice, December 15, 2022, https://www.brennancenter.org/our-work/policy-solutions/ending-fusion-center-abuses.

50 Martin de Bourmont and Jana Winter, "Exclusive: FBI Document Reveals Local and State Police Are Collecting Intelligence to Expand Terrorism Watch List," Yahoo News, February 7, 2020, https://www.yahoo.com/video/exclusive-fbi-document-reveals-local-and-state-police-are-collecting-intelligence-to-expand-terrorism-watch-list-100017370.html.

51 Complaint at ¶¶ 48–49, 64–65, Long v. Gourley, No. 23CV00080 (W.D. Okla. January 25, 2023), https://www.cair.com/wp-content/uploads/2023/01/LongComplaint.pdf. See also Michael McNutt, "Stopped 5 Times in 2 Months, Saadiq Long Seeks Answers and Protection with OKCPD Lawsuit," NonDoc.com, January 26, 2023, https://nondoc.com/2023/01/26/stopped-5-times-in-2-months-saadiq-long-seeks-answers-and-protection-with-okcpd-lawsuit.

52 *Long*, complaint at ¶ 65.

53 Parties' Joint Stipulation, *Long*, No. 23CV00080 (W.D. Okla. February 1, 2023), https://www.cair.com/wp-content/uploads/2023/02/Stipulation.pdf; and Ismail Allison, "CAIR-OK, CAIR LDF Welcome OKC Police's Decision to Instruct Its Officers to Disregard FBI Watchlist," CAIR, February 2, 2023, https://www.cair.com/press_releases/cair-ok-cair-ldf-welcome-okc-polices-decision-to-instruct-its-officers-to-disregard-fbi-watchlist.

54 CAIR, *Twenty Years Too Many*, 11. Long is probably not the only person detrimentally affected by the pipeline between the watch list and local police. While current statistics are not available, the former TSC director reported in 2010 that one-third of TSDB encounters arose from traffic stops. Doug Wyllie, "A Powerful Weapon for Police in the Post-9/11 World," Police1.com, September 10, 2010, https://www.police1.com/terrorism/articles/a-powerful-weapon-for-police-in-the-post-911-world-UxvMiVjXEgfFEt4u.

55 Elhady v. Piehota, 303 F. Supp. 3d 453, 459–60 (E.D. Va. 2017) (noting that plaintiffs had "experienced a number of other consequences, which they have reason to believe are attributable to their inclusion on the Watch List"; one plaintiff could not conduct wire transfers and another had three bank accounts closed without explanation); Kovac v. Wray, 363 F. Supp. 3d 721, 736 (N.D. Tex. 2019) (including allegation from one plaintiff that she had "been denied a credit card and bank loan due to the watchlist"); Long v. Barr, 451 F. Supp. 3d 507, 533n19 (E.D. Va. 2020) ("Plaintiff Long alleges that he . . . had a bank account frozen . . . because of his status."); El Ali v. Barr, 473 F. Supp. 3d 479, 497 (D. Md. 2020) (documenting plaintiffs' claim that "because [of] their placement in the TSDB and [because] watchlists is [*sic*] shared liberally, their bank accounts have been closed"); and *Khairullah*, complaint at ¶¶ 210–11 (including allegations from three plaintiffs that their accounts with Bank of America, Wells Fargo, Chase Bank, MoneyGram, and CashApp were closed due to their placement on the watch list).

56 *Elhady*, 303 F. Supp. 3d at 460. What mechanism a car dealership would have to obtain access to the list is unclear.

57 In addition to the watch list information disclosures described above, see Livia Albeck-Ripka and Miriam Jordan, "Identities of Thousands of Migrants Seeking Asylum in U.S. Posted in Error," *New York Times*, December 1, 2022, https://www.nytimes.com/2022/12/01/us/ice-migrants-privacy.html.

58 CAIR, *Twenty Years Too Many*, 7. See, e.g., Tanvir v. Tanzin, 894 F.3d 449, 456 (2d Cir. 2018) (noting that in October 2010, an FBI agent contacted Muhammad Tanvir and told him that "if he met with her and answered her questions, she would help remove his name from the No Fly List" (internal quotation marks omitted)); Fikre v. FBI, 23 F. Supp. 3d 1268, 1279 (D. Or. 2014) (detailing that in 2010, an FBI agent told the plaintiff that he could "take steps to remove [him] from the No-Fly List" if he agreed to become an informant for the FBI); and Latif v. Holder, 28 F. Supp. 3d 1134, 1145–46 (D. Or. 2014) (detailing instances where FBI agents offered to help remove three plaintiffs' names from the No Fly List if they became informants) (cited in *Khairullah*, complaint at ¶ 374).

59 *Elhady*, 303 F. Supp. 3d at 465; and Jeremy Scahill and Ryan Devereaux, "Watch Commander: Barack Obama's Secret Terrorist-Tracking System, by the Numbers," *Intercept*, August 5, 2014, https://theintercept.com/2014/08/05/watch-commander.

60 Government Accountability Office (hereinafter GAO), *Routinely Assessing Impacts of Agency Actions Since the December 25, 2009, Attempted Attack Could Help Inform Future Efforts*, May 2012, GAO Highlights, https://www.gao.gov/assets/gao-12-476.pdf. The GAO noted that at the time, "no single entity [was] accountable for routinely assessing the overall impacts the July 2010 Watchlisting Guidance [had] on the watchlisting community," nor was any government entity "routinely collecting and analyzing data needed to conduct such governmentwide assessments over time." GAO, *Routinely Assessing Impacts*, 12. Although the Information Sharing and Access Interagency Policy Committee (a forum that operates under the auspices of the White House and oversees how the federal government and its nonfederal partners share terrorism-related information) was undertaking an assessment of the watch-listing process, the GAO did not obtain information about how comprehensive this assessment would be or how frequently it would recur, nor did the office detail whether the assessment included an evaluation of the watch lists' accuracy. Federal Bureau of Investigation, *FBI Information Sharing and Safeguarding Report 2012*, DOJ, 2012, https://www.fbi.gov/stats-services/publications/national-information-sharing-strategy-1.

61 *Latif*, Sageman declaration at 7–8. See also Timme Bisgaard Munk, "100,000 False Positives for Every Real Terrorist: Why Anti-terror Algorithms Don't Work," *First Monday* 22, no. 9 (September 2017), https://firstmonday.org/ojs/index.php/fm/article/view/7126/6522.

62 Bernstein, "Hidden Costs of Terrorist Watch Lists," 478.

63 *Latif*, Sageman declaration at 13–14.

64 *Latif*, Sageman declaration at 17.

65 *Latif*, Sageman declaration at 9.

66 Privacy and Civil Liberties Oversight Board, "Current Oversight Projects," accessed September 12, 2023, https://www.pclob.gov/OversightProjects.

67 49 U.S.C. §§ 44903(j)(2)(C)(iii) and (G), 44926(a) (2020) (relating to the procedure to challenge delays to or prohibitions on boarding). This limited scope stands in contrast to Canada's equivalent of the No Fly List, under which travelers denied boarding are automatically notified if they are on that list and given the opportunity to request removal, rather than having to affirmatively submit an inquiry. Public Safety Canada, "Passenger Protect Program (PPP)," updated February 23, 2023, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/pssngr-prtct/pssngr-prtct-prgrm-en.aspx.

68 Defendants' Notice Regarding Revisions to DHS TRIP Procedures, Latif v. Lynch, No. 10CV00750 (D. Or. April 13, 2015); Kashem v. Barr, 941 F.3d 358, 366 (9th Cir. 2019) (describing revised 2015 DHS TRIP procedures); and Jibril v. Mayorkas, 20 F.4th 804, 810–11 (D.C. Cir. 2021) (quoting the letter received by the plaintiff).

69 Hina Shamsi, "The U.S. Government Is Putting Americans on Its No Fly List on a Hunch. And It Won't Even Tell Them Why," *Slate*, August 12, 2015, https://slate.com/news-and-politics/2015/08/the-u-s-government-is-putting-americans-on-its-no-fly-list-on-a-hunch-and-it-wont-say-why-they-are-grounded.html.

[70] The Privacy Act of 1974 could offer an additional path to obtain critical information, but major data systems have been exempted from its notification, access, and amendment requirements, foreclosing that approach. See, e.g., DHS Privacy Office, notice of proposal to update and expand Privacy Act system of records for the Automated Targeting System (DHS/CBP-006), 77 Fed. Reg. 30297, 30299 (May 22, 2012), https://www.federalregister.gov/d/2012-12396/p-24; DHS Privacy Office, notice of proposal to update and reissue Privacy Act system of records for Secure Flight (DHS/TSA-019), 78 Fed. Reg. 55270, 55274 (September 10, 2013), https://www.federalregister.gov/d/2013-21980/p-83; and DHS Privacy Office, notice of proposal to institute new DHS/CBP Privacy Act system of records titled CBP Intelligence Records System, or CIRS (DHS/CBP-024), 82 Fed. Reg. 44198, 44203 (September 21, 2017), https://www.federalregister.gov/d/2017-19718/p-114 (claiming similar exemptions for all CBP intelligence systems, including the Analytical Framework for Intelligence; see DHS, "DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI)," last modified March 31, 2023, https://www.dhs.gov/publication/analytical-framework-intelligence-afi). See also Rep. Bennie G. Thompson (chairman-designate, H. Comm. on Homeland Security), comments on DHS Privacy Office Privacy Act system of records notice for CBP Automated Targeting System, docket no. DHS-2006-0060, November 2, 2006, 2, https://www2.epic.org/privacy/travel/ats/atscom_bt122906.pdf. One scholar has recommended that Congress "amend the Privacy Act to eliminate or tighten the exemptions to its relevance, timeliness, completeness, and accuracy requirements." Bernstein, "Hidden Costs of Terrorist Watch Lists," 526.

[71] See, e.g., Complaint, Elhady v. Piehota, No. 16CV00375 (E.D. Va. April 5, 2016), https://clearinghouse.net/doc/97937 (lawsuit brought by 25 American Muslims challenging their presumed inclusion on the TSDB, their detention and harassment by law enforcement as a result, and the inadequacy of the established redress procedure through DHS TRIP); and Complaint, El Ali v. Barr, No. 18CV02415 (D. Md. August 8, 2018), https://clearinghouse.net/doc/111810 (complaint brought by 39 Muslim Americans challenging the watch-listing system under the Fourth and Fifth Amendments).

[72] See DHS Privacy Office, *2017 DHS Data Mining Report to Congress*, DHS, October 2018, 18, https://www.dhs.gov/sites/default/files/publications/2017-dataminingreport_0.pdf; and DHS Privacy Office, *2019 Data Mining Report to Congress*, DHS, December 2, 2020, 24, https://www.dhs.gov/sites/default/files/publications/2019_data_mining_report_final_12-2-20.pdf (describing how the programs "identify patterns indicative of terrorist or criminal activity" in concert with machine-driven predictive analytics programs). CBP's National Targeting Center and TSA's intelligence and analysis office carry out this function. The rules are reviewed before implementation and every quarter thereafter for as long as they are effective by DHS's Privacy Office, CRCL, and Office of the General Counsel, as well as the components' privacy offices, whose representatives have indicated in interviews that the reviews are thorough (though no audits of those processes are publicly available). GAO, *Border Security: CBP Aims to Prevent High-Risk Travelers from Boarding U.S.-Bound Flights, but Needs to Evaluate Program Performance*, January 2017, 10, 14, https://www.gao.gov/assets/gao-17-216.pdf; and Jonathan Cantor, *Privacy Impact Assessment Update for Secure Flight: Silent Partner and Quiet Skies*, DHS Privacy Office, April 19, 2019, 7, https://www.dhs.gov/sites/default/files/publications/pia-tsa-spqs018i-april2019_1.pdf.

[73] DHS Privacy Office, *2019 Data Mining Report*, 18.

[74] DOJ, *Predictive Analytics in Law Enforcement: A Report by the Department of Justice*, November 2014, 12, https://epic.org/wp-content/uploads/foia/doj/criminal-justice-algorithms/EPIC-16-06-15-DOJ-FOIA-20200319-Settlement-Production-pt1.pdf ("CBP's threat algorithms are generated through statistical modeling based on historical data. These predictive models are typically broader than user defined rules and are developed in response to more generalized threats."); and DHS Privacy Office, *2019 DHS Data Mining Report*, 14 ("ATS runs risk-based rules, predictive analytics, and queries to identify patterns indicative of terrorist or criminal activity.").

[75] A recent privacy impact assessment from I&A provides some information about how pattern detection could be conducted and operationalized by CBP from data within ATS in the context of known and suspected terrorists, but it is not clear that ATS's predictive modeling capabilities work similarly. Privacy Office, *Privacy Impact Assessment for DHS Data Analysis Tools,* DHS, June 13, 2023, 6, 18, https://www.dhs.gov/sites/default/files/2023-06/privacy-pia-dhsall055a-dat-june2023.pdf (noting that an analyst could use a data analysis tool to infer, for example, that "known or suspected terrorists are using stolen passports most frequently from country X to travel along route Y, with peak travel occurring in months A and B").

[76] Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Pub. L. No. 109-347, 120 Stat. 1884 (2006). See also SAFE Port Act §§ 203(a)(1)–(2) (requiring the secretary of homeland security, acting through the CBP commissioner, to "(1) identify and seek the submission of data related to the movement of a shipment of cargo through the international supply chain; and (2) analyze the data described in paragraph (1) to identify high-risk cargo for inspection").

[77] DHS Privacy Office, notice regarding system of records for the Automated Targeting System, 71 Fed. Reg. 64543, 64544 (November 2, 2006), https://www.federalregister.gov/documents/2006/11/02/06-9026/privacy-act-of-1974-system-of-records (revealing that DHS was using ATS to "assess[] the risk of international travelers"). DHS followed this notice the next year with a privacy impact assessment describing ATS's "primary purpose" as "targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States." Hugo Teufel III, *Privacy Impact Assessment for the Automated Targeting System*, DHS Privacy Office, August 3, 2007, 2, https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats_updated_fr_0.pdf.

[78] Thompson, comments on ATS system of records notice, 1–2 (asserting that DHS had failed to "adequately distinguish between CBP's legal authority and processes to use ATS to screen *cargo* from its legal authority and processes to screen *passengers*" (emphasis added) and expressing concern that ATS's application to passengers "may constitute violations of the privacy and civil liberties of U.S. citizens and lawful permanent residents"). See also Ellen Nakashima and Spencer S. Hsu, "U.S. Plans to Screen All Who Enter, Leave Country," *Washington Post*, November 3, 2006, https://www.washingtonpost.com/wp-dyn/content/article/2006/11/02/AR2006110201810_pf.html (quoting a congressional aide as saying, "ATS started as a tool to prevent the entry of drugs with cargo into the U.S. We are not aware of Congress specifically legislating to make this expansion possible").

[79] See S. Comm. on Appropriations, Department of Homeland Security Appropriations Bill, 2015, S. Rep. No. 113-198 (2014), 49, https://www.congress.gov/113/crpt/srpt198/CRPT-113srpt198.pdf. The Senate Appropriations Committee included identical language in its reports accompanying the homeland security appropriations bills for fiscal years 2016 and 2017. S. Comm. on Appropriations, Department of Homeland Security Appropriations Bill, 2016, S. Rep. No. 114-68 (2015), 43, https://www.congress.gov/114/crpt/srpt68/CRPT-114srpt68.pdf; and S. Comm. on Appropriations, Department of Homeland Security Appropriations Bill, 2017, S. Rep. No. 114-264 (2016), 46, https://www.congress.gov/114/crpt/srpt264/CRPT-114srpt264.pdf. See also H. Comm. on Appropriations, Department of Homeland Security Appropriations Bill, 2014, H. Rep. No. 112-91 (2013), 26, https://www.congress.gov/113/crpt/hrpt91/CRPT-113hrpt91.pdf.

[80] See Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, January 2016, 9, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf (noting that the use of "spurious correlations" uncovered through data

mining to inform decision-making without understanding their basis may lead to unintended consequences that harm individuals); and Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, White House, October 2022, 16–17, 24–25, 41–42, https://www.whitehouse.gov/ostp/ai-bill-of-rights (detailing potential harms when systems powered by artificial intelligence are not properly tested and are deployed without effective safeguards).

81 Jonathan Cantor, *Privacy Impact Assessment Update for the Automated Targeting System*, DHS Privacy Office, January 13, 2017 (hereinafter *PIA Update for ATS*), 3, 78, https://www.dhs.gov/sites/default/files/2022-07/privacy-pia-cbp006-ats-july2022_0.pdf (noting that ATS ingests data from TECS).

82 See 19 C.F.R. § 122.49d; DHS Privacy Office, notice of proposal to update and expand ATS system of records (DHS/CBP-006), 77 Fed. Reg. 30298; and Edward Hasbrouck, "What's in a Passenger Name Record (PNR)?," *Practical Nomad* (blog), accessed September 12, 2023, https://hasbrouck.org/articles/PNR.html (describing the breadth of revealing information contained in passenger name records, or PNRs). See also Seth M. Stodder, "Rethinking Borders: Securing the Flows of Travel and Commerce in the Twenty-First Century," in Lawson, Bersin, and Kayyem, *Beyond 9/11*, 91 (observing that after 9/11, Congress required airlines to make PNRs available to CBP, allowing the agency to "begin performing ever-more sophisticated analysis of the data").

83 Sen. Ron Wyden to Chris Magnus (commissioner, CBP), September 15, 2022, https://www.wyden.senate.gov/imo/media/doc/Wyden%20letter%20to%20CBP%20on%20border%20searches%20of%20devices.pdf.

84 DHS can access DMV records through both direct requests and access to government databases containing driver's license data through the National Law Enforcement Telecommunications System, or Nlets, to which ATS has access through TECS. DHS can also access this data through data brokers. See Nina Wang et al., *American Dragnet: Data-Driven Deportation in the 21st Century*, Georgetown Law Center on Privacy and Technology, May 10, 2022, 30, 34, https://americandragnet.org/sites/default/files/American_Dragnet_report_English_final.pdf; and Jonathan Cantor, *Privacy Impact Assessment for the TECS System: Platform*, DHS Privacy Office, August 12, 2016 (hereinafter *PIA for TECS Platform*), 5, https://www.dhs.gov/sites/default/files/publications/DHS-PIA-ALL-021%20TECS%20System%20Platform.pdf.

85 *PIA Update for ATS*, 3, 78, https://www.dhs.gov/sites/default/files/2022-07/privacy-pia-cbp006-ats-july2022_0.pdf; and 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.

86 DHS Privacy Office, *2019 Data Mining Report*, 23–24; and Cantor, *PIA Update for ATS*, 103 (announcing an effort to screen immigrants and refugees through ATS). CBP also runs TSA's rules in ATS to facilitate Secure Flight, TSA's air travel screening program. Cantor, *PIA Update for Secure Flight: Silent Partner and Quiet Skies*, 1.

87 See Cantor, *PIA Update for ATS*, 3–5, 9–10, 12–13.

88 See GAO, *Data Mining: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism*, September 2011, 32, https://www.gao.gov/assets/gao-11-742.pdf (recommending that the DHS chief information officer and chief procurement officer work together on components' compliance with departmental policies); GAO, *Secure Flight: TSA Should Take Additional Steps to Determine Program Effectiveness*, September 2014, 27–28, https://www.gao.gov/assets/gao-14-531.pdf (stating that TSA should develop measures to address performance aspects with respect to goals for screening measures); GAO, *CBP Aims to Prevent High-Risk Travelers from Boarding U.S.-Bound Flights*, 24 (reporting that CBP has not fully assessed the overall efficacy of its predeparture programs "using performance measures and baselines"); and GAO, *Aviation Security: TSA Coordinates with Stakeholders on Changes to Screening Rules but Could Clarify Its Review Processes and Better Measure Effectiveness*, November 2019, 17, https://www.gao.gov/assets/gao-20-72.pdf (recommending that TSA should explore additional data sources to measure the effectiveness of Quiet Skies and Silent Partner rules).

89 Federal Agency Data Mining Reporting Act of 2007, Pub. L. No. 110-53, 121 Stat. 362 (2007) (codified at 42 U.S.C. § 2000ee-3); and DHS, "DHS Data Mining Reports," last modified August 31, 2023, https://www.dhs.gov/publication/dhs-data-mining-reports.

90 DHS published an initial data-mining report in 2006, prior to the statute's passage; its first formal data-mining report was published in 2007, and the last one that is publicly available is the compiled report for 2020 and 2021, which DHS released in August 2023. DHS, "DHS Data Mining Reports."

91 These examples are from the ATS passenger and land module sections. One example is identical in the 2017 and 2018 reports, and all examples included in the 2019 report are duplicated from the 2018 report. It is unclear whether any of the use cases included in the compiled report for 2020 and 2021 involved ATS's risk assessment capabilities. DHS, "DHS Data Mining Reports."

92 DHS Privacy Office, *2014 Data Mining Report to Congress*, DHS, January 2015, 19, https://www.dhs.gov/sites/default/files/publications/2014%20DHS%20Data%20Mining%20Report%20Signed_1.pdf.

93 OIG, *TSA Needs to Improve Management of the Quiet Skies Program (Redacted)*, DHS, November 25, 2020, 11, https://www.oig.dhs.gov/sites/default/files/assets/2020-11/OIG-21-11-Nov20-Redacted.pdf (recommending that TSA develop procedures to ensure the reliability of Quiet Skies data); and GAO, *Aviation Security*, 17.

94 Lawson, "Trusted and the Targeted," 112.

95 Melissa del Bosque, "Secretive CBP Counterterrorism Teams Interrogated 180,000 U.S. Citizens over Two-Year Period," *Intercept*, September 4, 2021, https://theintercept.com/2021/09/04/cbp-border-tactical-terrorism-response-teams; and CBP, "Tactical Terrorism Response Team" (redacted), DHS, accessed September 12, 2023, 3, https://www.aclu.org/sites/default/files/field_document/exhibit_h-j.pdf (see page 24 of the compiled document).

96 *Raising the Standard: DHS's Efforts to Improve Aviation Security Around the Globe, Hearing Before the Subcomm. on Transportation and Protective Security of the H. Comm. on Homeland Security*, 115th Cong. (2017) (statement of Craig Lynes, director of global compliance, TSA, and Todd Owen, executive assistant commissioner, Office of Field Operations, CBP), https://www.govinfo.gov/content/pkg/CHRG-115hhrg28417/html/CHRG-115hhrg28417.htm; del Bosque, "Secretive CBP Counterterrorism Teams" (noting that TTRTs "operate at 79 ports of entry and in all 20 of the Border Patrol sectors nationwide"); and CBP, "Protecting the U.S. from Biothreats: It Starts with Policy," DHS, March 27, 2023, https://www.cbp.gov/newsroom/spotlights/protecting-us-biothreats-it-starts-policy.

97 del Bosque, "Secretive CBP Counterterrorism Teams."

98 Brian Dodwell and Paul Cruickshank, "A View from the CT Foxhole: An Interview with Kevin McAleenan, Commissioner of U.S. Customs and Border Protection," *CTC Sentinel* 11, no. 18 (September 2018), https://ctc.westpoint.edu/view-ct-foxhole-interview-kevin-mcaleenan-commissioner-u-s-customs-border-protection (quoting former acting Secretary of Homeland Security Kevin McAleenan as stating that TTRTs were "a conscious effort by the Office of Field Operations . . . to take advantage of those instincts and encounters that our officers have with travelers to make decisions based on risk for people that might not be known on a watch list [or] might not be a known security threat"); and del Bosque, "Secretive CBP Counterterrorism Teams."

99 CBP, "Area Port of Entry [redacted] Standard Operating Procedures: Tactical Terrorism Response Team," January 16, 2017, 1–2, https://www.aclu.org/sites/default/files/field_document/exhibit_h-j.pdf (see pages 32–33 of the compiled document).

[100] del Bosque, "Secretive CBP Counterterrorism Teams."

[101] del Bosque, "Secretive CBP Counterterrorism Teams."

[102] ACLU of Northern California to DHS OIG, CRCL, and CBP, Re: Policies and Practices Related to the Electronic Device Search of U.S. Citizen at San Francisco International Airport, March 28, 2019, 2–3, https://www.aclunc.org/docs/ACLU-NC_2019-03-28_Letter_re._Electronic_Device_Search_SFO.pdf; and Andreas Gal (@andreasgal), "No One Should Have to Travel in Fear," Medium, April 2, 2019, https://medium.com/@andreasgal/no-one-should-have-to-travel-in-fear-b2bff4c460e5.

[103] Dana Salvano-Dunn (director, compliance branch, CRCL) to Chris Magnus (commissioner, CBP) and Scott K. Falk (chief counsel, CBP), memorandum, Re: Tactical Terrorist Response Team Complaint Nos. 19-11-CBP-0592, 20-06-CBP-0469, 20-10-CBP-0814, 20-11-CBP-0928, 21-04-CBP-0219, 21-07-CBP-0381, 001058-21-CBP, 001557-21-CBP, 002245-21-CBP, 002341-21-CBP, and 002610-22-CBP, April 5, 2022, 1, https://www.dhs.gov/sites/default/files/2022-07/2022.04.05%20CRCL%20Retention%20Memo%20to%20CBP%20-%20Tactical%20Terrorist%20Response%20Team%20-%20Redacted_508.pdf.

[104] Electronic devices can be searched to uncover evidence of crime, information relevant to inadmissibility, or "intentions upon entry." McAleenan, CBP Directive No. 3340-049A: Border Search of Electronic Devices, 1; and Hillel Smith, *Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment?*, Congressional Research Service, March 17, 2021, https://crsreports.congress.gov/product/pdf/LSB/LSB10387. The devices and data seized from them are available to DHS's Office of Intelligence and Analysis, which can use the data for additional purposes. Spencer Reynolds and Faiza Patel, *A New Vision for Domestic Intelligence: Fixing Overbroad Mandates and Flimsy Safeguards*, Brennan Center for Justice, March 30, 2023, 5, https://www.brennancenter.org/our-work/policy-solutions/new-vision-domestic-intelligence.

[105] See Ryan Singel, "U.S. Airport Screeners Are Watching What You Read," *Wired*, September 20, 2007, https://www.wired.com/2007/09/u-s-airport-screeners-are-watching-what-you-read.

[106] OIG, *CBP Continues to Experience Challenges Managing Searches of Electronic Devices at Ports of Entry (Redacted)*, DHS, September 23, 2021, https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-63-Sep21-Redacted.pdf; and OIG, *CBP's Searches of Electronic Devices at Ports of Entry (Redacted)*, DHS, December 3, 2018, https://www.oig.dhs.gov/sites/default/files/assets/2018-12/OIG-19-10-Nov18.pdf. CBP carried out over 45,000 electronic device searches in fiscal year 2022 alone; as of 2018, 20 percent of device searches were conducted on U.S. citizens. CBP, "CBP Enforcement Statistics Fiscal Year 2023," DHS, accessed September 12, 2023, https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics; and Geneva Sands, "Searches of Travelers' Electronic Devices Up Nearly 60 Percent," ABC News, January 5, 2018, https://abcnews.go.com/US/searches-travelers-electronic-devices-60-percent/story?id=52171977.

[107] Jana Winter, "Operation Whistle Pig: Inside the Secret CBP Unit with No Rules That Investigates Americans," Yahoo News, December 11, 2021, https://news.yahoo.com/operation-whistle-pig-inside-the-secret-cbp-unit-with-no-rules-that-investigates-americans-100000147.html.

[108] Jana Winter, "CBP Unit That Spied on Journalists and Lawmakers Is Monitoring American Protesters," Yahoo News, January 26, 2022, https://news.yahoo.com/cbp-unit-that-spied-on-journalists-and-lawmakers-is-monitoring-american-protestors-100039195.html.

[109] See Cantor, *PIA for TECS Platform*, 2 (describing TECS's dual information-sharing and case management functions). TECS used to stand for Treasury Enforcement Communications System but is now a stand-alone name, not an acronym. For a full list of databases stored on or accessible through TECS, including CBP's Advance Passenger Information System (APIS) and Border Crossing Information (BCI) system, the TSDB, Nlets, and more, see Cantor, *PIA for TECS Platform*, 33–34.

[110] See Mary Ellen Callahan, *Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing*, DHS Privacy Office, December 22, 2010 (hereinafter *PIA for TECS CBP Primary and Secondary*), 8–9, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf.

[111] OIG, *DHS Has Controls to Safeguard Watchlist Data*, DHS, July 25, 2022, 4, https://www.oig.dhs.gov/sites/default/files/assets/2022-07/OIG-22-53-Jul22.pdf; GAO, *Border Security: DHS's Efforts to Modernize Key Enforcement Systems Could Be Strengthened*, December 2013, 3, https://www.gao.gov/assets/gao-14-62.pdf; Cantor, *PIA for TECS Platform*, 2, 5, 12 (noting that TECS has access to APIS, BCI, NCIC, and the watch lists through the DHS Watchlist Service); and Joan Friedland, *Untangling the Immigration Enforcement Web: Basic Information for Advocates About Databases and Information-Sharing Among Federal, State, and Local Agencies*, National Immigration Law Center, September 2017, 7, https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf (noting that "NCIC contains civil records in addition to criminal ones"). DHS has exempted TECS records from notification, access, and amendment provisions of the Privacy Act, as well as the act's requirement to maintain records used to make determinations about individuals "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." DHS Privacy Office, notice of revised Privacy Act system of records for TECS (DHS/CBP-011), 73 Fed. Reg. 77778, 77782 (December 19, 2008), https://www.federalregister.gov/d/E8-29807/p-86; and 5 U.S.C. § 552a(e)(5) (2000).

[112] Cantor, *PIA for TECS Platform*, 2, 46.

[113] See Ryan Devereaux, "Faith Under Fire: A Pastor's Legal Fight Against CBP Exposes a Reckless Surveillance Operation," *Intercept*, March 6, 2022, https://theintercept.com/2022/03/06/cbp-border-surveillance-migrant-caravan; Complaint, Guan v. Mayorkas, No. 19CV06570 (E.D.N.Y. November 20, 2019), https://cbpabusestest2.files.wordpress.com/2020/06/guan.complaint.pdf; and OIG, *CBP Targeted Americans Associated with the 2018–2019 Migrant Caravan*, September 20, 2021, 11, https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-62-Sep21.pdf.

[114] Douša v. DHS, 2023 U.S. Dist. LEXIS 48066, *58–63, 70–71 (S.D. Cal. 2023).

[115] Brian Hauss, "Documents Shed Light on Border Laptop Searches," ACLU, September 9, 2013, https://www.aclu.org/blog/national-security/privacy-and-surveillance/documents-shed-light-border-laptop-searches; and Susan Stellin, "The Border Is a Back Door for U.S. Device Searches," *New York Times*, September 9, 2013, https://www.nytimes.com/2013/09/10/business/the-border-is-a-back-door-for-us-device-searches.html.

[116] Cantor, *PIA for TECS Platform*, 15, 17; and Callahan, *PIA for TECS CBP Primary and Secondary*, 14. In his case challenging DHS's practice of questioning Muslim travelers about their religious beliefs and observances, for instance, Imam Kariye challenged the storage of travelers' responses in TECS for future use. Sarah Taitz, "Customs and Border Protection Is Singling Out Muslim Travelers for Invasive Religious Questioning," ACLU, March 24, 2022, https://www.aclu.org/news/religious-liberty/customs-and-border-protection-is-singling-out-muslim-travelers-for-invasive-religious-questioning; and *Kariye*, complaint at ¶¶ 27–29.

[117] Congress should also restrict DHS's purchase of commercial data in circumstances wherein it would otherwise need to obtain a warrant, subpoena, or court order to obtain the data. See Fourth Amendment Is Not for Sale Act, S. 1265, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1265/text; and American Data Privacy and Protection Act, H.R. 8152, 117th Cong.

(2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

118 Although outside the scope of this report, Congress's assessment should include the NCTC's TIDE repository, which is used for a range of counterterrorism purposes and is plagued by many of the same issues as the TSDB.

119 The Brennan Center has recommended that Congress create such a special inspector general for audits of the national network of fusion centers. German, Levinson-Waldman, and Mueller-Hsia, *Ending Fusion Center Abuses*, 11.

120 See National Institute of Standards and Technology (hereinafter NIST), "AI Risk Management Framework," Department of Commerce, accessed September 12, 2023, https://www.nist.gov/itl/ai-risk-management-framework (providing guidance on "artificial intelligence systems," defined as "an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments," a definition that encompasses TSA's Secure Flight and ATS, among other systems); Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights*; Exec. Order No. 14091, "Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," 88 Fed. Reg. 10825 (February 22, 2023), https://www.govinfo.gov/app/details/FR-2023-02-22/2023-03779; Alejandro Mayorkas (secretary, DHS), memorandum, Re: Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components, August 8, 2023, https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_139-06-acquistion-use-ai-technologies-dhs-components.pdf; and DHS, "DHS Announces New Policies and Measures Promoting Responsible Use of Artificial Intelligence," news release, September 14, 2023, https://www.dhs.gov/news/2023/09/14/dhs-announces-new-policies-and-measures-promoting-responsible-use-artificial. See also Reva Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, NIST, March 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

121 This recommendation is not intended to take a position on the applicability of such mechanisms to non-U.S. persons.

122 See, e.g., Dustin Volz and Warren P. Strobel, "NSA Recommends Dropping Phone-Surveillance Program," *Wall Street Journal*, April 24, 2019, https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247.

ABOUT THE AUTHORS

▶ **Rachel Levinson-Waldman** is managing director of the Brennan Center's Liberty and National Security Program, where she works to shed light on the government's use of surveillance technologies and authorities and its collection and use of data for law enforcement and intelligence purposes. Levinson-Waldman has authored articles and reports on topics including DHS's counterterrorism initiatives, the government's use of social media, and Fourth Amendment implications of public space surveillance. She has written and provided expert input for publications including the *Guardian*, the *Washington Post*, *Wired*, the *Atlantic*, and the *New Republic*. She is a graduate of Williams College and the University of Chicago Law School.

▶ **José Guillermo Gutiérrez** is a program associate in the Brennan Center's Liberty and National Security Program. Prior to joining the Brennan Center, he was a domestic policy intern at the Biden for President campaign and a research volunteer on the Biden-Harris Presidential Transition. Gutiérrez is a graduate of the University of Southern California.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect constitutional values and the rule of law, using research, innovative policy recommendations, litigation, and public advocacy. The program focuses on reining in excessive government secrecy, ensuring that counterterrorism authorities are narrowly targeted to the terrorist threat, and securing adequate oversight and accountability mechanisms.

ACKNOWLEDGMENTS

The Brennan Center gratefully acknowledges CS Fund/Warsh-Mott Legacy and Media Democracy Fund for their generous support of our work. This is an independent Brennan Center publication; the opinions expressed are those of the authors and do not necessarily reflect the views of our supporters.

The authors are grateful to members of the Brennan Center's Liberty and National Security team who provided critical advice, input, and research, including Michael German, Liza Goitein, Faiza Patel, Spencer Reynolds, and Alia Shahzad, as well as interns Danielle Recanati, Harry Reis, Sam Rudovsky, and Sherry Tseng. The authors are also grateful to the outside experts who offered thoughtful feedback and insights, including Gadeir Abbas, Emily Berman, Joan Friedland, Edward Hasbrouck, the team at Paul Hastings LLP, Chris Rickerd, Hina Shamsi, Patrick Toomey, and current and former government officials who wish to remain anonymous. Michael Waldman and John Kowal provided guidance and support. Finally, this report benefited from the conscientious editing and communications assistance of Marcelo Agudo, Julian Brookes, Zachary Laub, Janet Romero-Bahari, Stephanie Sykes, and Alden Wallace.

BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
www.brennancenter.org