RESEARCH REPORT

BRENNAN CENTER FOR JUSTICE

DHS AT 20: AN AGENDA FOR REFORM

A Course Correction for Homeland Security

Curbing Counterterrorism Abuses

By Faiza Patel, Rachel Levinson-Waldman, and Harsha Panduranga
PUBLISHED APRIL 20, 2022

Brennan Center for Justice at New York University School of Law

Table of Contents

Abbreviations 3

Introduction 4

I. Counterterrorism Partnerships with State and Local Authorities 5

Fusion Centers 5

Office of Intelligence and Analysis 7

Violence Prevention Programs and Partnerships 9

II. Data Collection, Risk Assessments, and Profiling 10

Data Collection 10

Data Storage and Analysis 12

Risk Assessments 14

Religious and National Origin Profiling 15

III. Oversight 17

Office for Civil Rights and Civil Liberties 17

Privacy Office 20

Office of Inspector General 21

IV. Recommendations 23

Strengthen Safeguards Against Profiling 23

Protect Privacy and Free Expression 23

Evaluate Efficacy 24

Ensure Meaningful Transparency 24

Foster Robust Oversight 24

Conclusion 25

Endnotes 26

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform and revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at
www.brennancenter.org

Abbreviations

AFI Analytical Framework for Intelligence

ATS Automated Targeting System

CBP U.S. Customs and Border Protection

CETC Current and Emerging Threats Center

CP3 Center for Prevention Programs and Partnerships

CRCL DHS Office for Civil Rights and Civil Liberties

CVE Countering Violent Extremism

DHS U.S. Department of Homeland Security

DOJ U.S. Department of Justice

ESTA Electronic System for Travel Authorization

FBI Federal Bureau of Investigation

GAO U.S. Government Accountability Office

HART Homeland Advanced Recognition Technology database

I&A DHS Office of Intelligence and Analysis

ICE U.S. Immigration and Customs Enforcement

ISE Information Sharing Environment

MIAC Maine Information and Analysis Center

NSA National Security Agency

OIG DHS Office of Inspector General

OIRA White House Office of Information and Regulatory Affairs

OPS DHS Office of Operations Coordination

PCR privacy compliance review

PIA privacy impact assessment

SAR suspicious activity report

SORN system of records notice

SPOT Screening of Passengers by Observation Techniques

TECS DHS information-sharing platform
(formerly the Treasury Enforcement Communications System)

TRIP Traveler Redress Inquiry Program

TSA Transportation Security Administration

TSDB Terrorist Screening Database

Introduction

In the wake of 9/11, Congress established a new cabinet agency with a singular mission: to keep the country safe from terrorism. The Department of Homeland Security (DHS) brought together 22 agencies with disparate functions under one roof. Two decades on, it struggles to carry out its work effectively and equitably.

Experts and advocates have scrutinized recurring abuses in DHS's enforcement of immigration law and proposed robust reforms.[1] DHS's counterterrorism initiatives, by contrast, often operate under the public's radar. So, too, do its travel and immigration screening programs. Yet these activities touch the lives of millions of Americans every day.

The department has aggressively targeted Muslims, communities of color, and social justice movements in the name of security. It conceals information about its vast databases and intrusive surveillance technologies. And it often embarks on ventures that implicate Americans' privacy, civil rights, and civil liberties without even establishing or measuring their usefulness.

These problems have long festered due to a dangerous combination of broad authorities, weak safeguards, and insufficient oversight. The Trump administration brought them to the fore. DHS agents enforced the president's ban on travelers from half a dozen Muslim-majority countries, wrenched children from parents at the southern border, escalated violence at protests from Washington, DC, to Portland, Oregon, spied on journalists and activists, and menaced immigrant communities from New York to New Mexico.

For most of its existence, DHS focused too narrowly on so-called international terrorism. It construed this mandate to include the activities of American Muslims, regardless of whether they had connections to foreign terrorist groups.[2] Only belatedly is DHS turning its attention to domestic terrorism, particularly far-right political violence. In 2021, Secretary Alejandro Mayorkas announced that the department will increase grants for state and local governments and add a division to its intelligence arm.

But simply shifting its focus is not enough. The Biden administration has yet to critically evaluate the department's post-9/11 missteps or fix the systems that have entrenched them. A course correction is critical.

With the Homeland Security Act of 2002, Congress tasked the new department with keeping the country safe from terrorist attacks. But DHS is far from the sole federal agency with a counterterrorism mission. The Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Office of the Director of National Intelligence, among other agencies, carry the lion's share of responsibility for it. DHS carved out a role for itself in two main areas: partnerships with state, local, tribal, and territorial authorities and screening of travelers and immigrants.

Section I of this report identifies the agency's counterterrorism collaborations with state and local authorities and private firms. These programs have routinely surveilled American Muslims, traumatizing entire communities and casting them as hotbeds of terrorism. DHS agents have deployed these very tools against protestors, activists, and journalists.

Section II turns to travel and immigration screening programs. DHS has accumulated vast stores of information about people who travel into, out of, and over the United States. The Transportation Safety Administration (TSA) and Customs and Border Protection (CBP), among other DHS components, use this data to draw inferences about them, document their movements, and subject them to warrantless searches and interrogations. Agents do all of this without suspicion of potential wrongdoing. Unsurprisingly, reports of religious or ethnic profiling are common.

Section III analyzes DHS's oversight infrastructure. Three primary offices — the Privacy Office, the Office for Civil Rights and Civil Liberties (CRCL), and the Office of Inspector General (OIG) — have curbed some of the department's transgressions. But they have allowed many other civil rights and civil liberties violations to continue.

Finally, this report identifies five avenues for reform: stronger safeguards against profiling; better protections for privacy and free expression; rigorous evaluations of program efficacy; meaningful transparency about data holdings and the implications DHS programs have for civil rights and civil liberties; and more robust internal oversight. Forthcoming Brennan Center reports will delve into these recommendations in greater detail.

The secretary of homeland security can — and should — make these changes now. The ease with which President Donald Trump weaponized DHS against both immigrants and citizens demonstrates that there are not sufficient safeguards against abuse. It is time for DHS to rein in its discriminatory and ineffective approaches and prevent new ones from being institutionalized.

I. Counterterrorism Partnerships with State and Local Authorities

DHS's counterterrorism efforts have long depended on cooperation with state and local authorities and private actors, in particular through federally established information-sharing mechanisms, the dissemination of terrorism analyses to state and local authorities, and violence prevention initiatives. These programs, which have repeatedly targeted minority communities and protest movements, have produced little discernible counterterrorism value.

Fusion Centers

Fusion centers were created after 9/11 as hubs for sharing information among federal law enforcement and intelligence agencies, their nonfederal counterparts, and nongovernmental partners. The centers are run by state and local governments and supported by the federal government, most significantly through DHS's Office of Intelligence and Analysis (I&A).[3] They obtain and distribute information from a wide array of sources — including law enforcement, U.S. military, and homeland security databases; emergency response and public health agencies; suspicious activity reports (SARs) generated by members of the public and the private sector; and public records and commercial data aggregators — under the theory that this material can be pooled to anticipate terrorist attacks.[4] Today, 80 fusion centers are funded by a combination of direct federal spending, federal grants, and state and local investments.[5] They are staffed primarily by local and state law enforcement, alongside DHS personnel and occasional liaisons from sectors such as fire departments, public health and cybersecurity agencies, and state national guards.[6]

Sharing credible information about actual threats of violence is vital. But fusion centers have repeatedly disseminated false, biased, and unreliable information and focused disproportionate attention on minority communities and protest movements — all with minimal demonstrated security benefit.

These problems have been well documented for a decade. In 2012, a two-year-long bipartisan Senate investigation of fusion centers concluded that the system had "yielded little, if any, benefit to federal counterterrorism intelligence efforts." Rather, the Senate report found, fusion centers produced reports that were "oftentimes shoddy" and "rarely timely."[7] The report highlighted the scrutiny that centers had imposed on Muslim groups in particular for benign activities such as hosting events on subjects like marriage and "positive parenting."[8] One fusion center report released in 2009, just prior to the period reviewed by Senate investigators, even depicted routine advocacy by Muslim civil rights groups as support for terrorism.[9]

Reports of such problems have persisted in the decade since the Senate report. A Chicago-area fusion center reportedly sent DHS and the FBI alerts that it knew to be unreliable about conversations and picture-taking by people who appeared to be "Arabic" or "Middle Eastern."[10] A Boston-area fusion center scanned social media for #BlackLivesMatter, #MuslimLivesMatter, and commonplace Arabic words.[11] Centers have also targeted racial justice activists and people celebrating Juneteenth, disseminating information about event organizers and attendees to law enforcement and intelligence agencies and tracking the locations of people posting the Black Lives Matter hashtag.[12] Other targets have included environmental activists and people demonstrating on issues ranging from women's rights to the government response to Hurricane Maria in Puerto Rico.[13] Some fusion center reporting has veered into patently irrelevant matters, pursuing issues such as the "Criminal and Violent Extremist Use of Emojis," alleged musical collaborations between "Subscribers of Black Extremism" and the "Indigenous Anarchist Federation," and the release of a Harry Potter mobile phone game.[14]

Disseminating biased and unreliable information to law enforcement poses serious risks to the people identified as threats.[15] As Michael German, a Brennan Center fellow and former FBI agent, told the *Intercept* about inaccurate fusion center reporting about protests and protesters: "I always try to read these and put myself in the shoes of a young police officer that doesn't know anything about this subject. . . . All this tells me to do is be very afraid of these people and imagine the worst of anything that they do."[16]

Fusion centers are supposed to implement a long list of oversight and compliance mechanisms to receive federal support. (They are also subject to the laws of the state or municipality in which they are located.) Specifically, fusion centers are required to maintain and publish policies covering privacy, civil rights, and civil liberties, and they must conduct reviews in accordance with federal guidelines to ensure that those policies are sufficiently robust and that they are adhered to. Indeed, federal guidance is detailed and voluminous.[17]

Case Study: The Maine Fusion Center

>> Documents released as part of a June 2020 hack of law enforcement websites known as BlueLeaks showed that the Maine Information and Analysis Center (MIAC) tracked the locations of and participants connected to racial justice activism events as part of daily reporting on "civil unrest."[18] The targets included Black Lives Matter protests and a vigil sponsored by a community organization promoting diversity.[19] A whistleblower has sued MIAC claiming that he was demoted after pointing out that the agency was collecting data on people who had applied to buy guns, as well as on protesters and employees of a camp that brings together Israeli and Arab teens.[20]

MIAC also disseminated baseless warnings of potential violence at racial justice protests to local police departments, cautioning police across the state that websites "rumored to be managed by Antifa" were recruiting professional protesters to "agitate and commit violent acts," and that organizers were using those websites to "facilitate payments to violent agitators."[21] These warnings originated from FBI and DHS reports that were based on unreliable or irrelevant sources — namely, a satirical website called Protest Jobs, which purported to offer rioters for hire, and the social media posts of far-right provocateurs. The type of FBI reports on which MIAC relied would typically note that they contained data that had not been "fully evaluated, integrated with other information, interpreted or analyzed"; MIAC's amplification of noncredible material illustrates the perils of an intelligence infrastructure that emphasizes the dissemination of information with few meaningful safeguards to verify its reliability or relevance.

Moreover, MIAC itself is known to operate with little oversight: it appoints its own oversight committee, which hid its membership — now reported to be comprised almost entirely of former law enforcement officials — for nearly a decade.[22] A bipartisan bill to close MIAC passed the state house in 2021 but failed in the senate.[23]

In practice, however, these measures are inadequate. While DHS's intelligence unit does run an annual assessment of fusion centers, it relies almost exclusively on self-reported data to check compliance, frequently resulting in findings of near-perfect compliance even as abusive practices continue.[24] The few public disclosures that exist suggest that the combination of fusion center self-reporting and state and local compliance mechanisms fails to make for an effective oversight infrastructure:

- The Austin-area fusion center is required to undergo external audits reviewed by the city's Public Safety Commission.[25] But the commission reportedly received only a single "two page, non-substantive" report from its 2014 peer-to-peer review with an El Paso counterpart; according to researchers who reviewed the document, it said little more than that the exercise was "very productive."[26] The next year, the commission was notified of a peer review with the Boston-area fusion center but received no written materials from the review, leaving it without a means to conduct effective oversight.[27] Both the Austin- and Boston-area fusion centers are among those responsible for abuses related to spying on Black activists and community groups and monitoring the internet for constitutionally protected speech presumed to be associated with Muslims.[28]

- A 2014 peer-to-peer exchange between the Oregon and Idaho fusion centers was similarly vague, finding that the Oregon center's information-sharing relationships were of "significant value" but offering no concrete details in support of the claim and stating with little analysis that both centers had made protecting privacy and civil liberties "a priority."[29] In 2021, Oregon community organizers and social justice advocates sued the state's Department of Justice, alleging that the fusion center had routinely engaged in "surveillance of . . . individuals engaged in innocuous and constitutionally protected activity, including peaceful assemblies."[30]

- Open the Government, a nonpartisan coalition, reviewed years of audits from the Chicago-area fusion center and found that its compliance division recommended "only small changes in . . . internal regulations, but a near-blanket rubber stamp" of the center's activities, even as the center disseminated biased intelligence reports.[31]

- When Massachusetts attempted in 2018 to audit the efficacy of the Commonwealth Fusion Center, its primary fusion center, the center refused to give the auditor access to its systems or to basic information on its operations.[32]

The weak information-sharing standards established by the federal government bear much of the blame for the fusion centers' subpar performance. Through a computer system called the Information Sharing Environment (ISE), fusion centers disseminate suspicious activity reports, which document observed behavior potentially related to terrorism that is reported by citizens, private-sector personnel, government officials, or law enforcement.[33] As detailed in an earlier Brennan Center report, this system jettisoned time-tested standards by functionally exempting the ISE from 28 C.F.R. Part 23, the federal rule requiring that the inclusion of personally identifiable information in criminal

intelligence databases be supported by reasonable suspicion of criminal conduct or activity — essentially defining SARs as material not subject to this requirement.[34]

Instead of evaluating whether a suspicious activity report is connected to a potential crime, fusion center staff determine whether a report contains a "potential nexus to terrorism." They do so by evaluating whether the report is "reasonably indicative of pre-operational planning associated with terrorism," including such common activities as taking photographs, looking through binoculars, writing notes, or asking questions about an event or building.[35] If the report meets this overbroad standard, it is uploaded to the system, where it can be accessed by other fusion centers along with the FBI and DHS, and is disseminated to a range of other law enforcement agencies.[36]

As a consequence, the majority of information collected by fusion centers has nothing to do with terrorism.[37] According to DHS, 100,000 SARs were submitted between 2010 and 2017, of which 35,000 were found to have some link to terrorism — an immense but unsurprising number given the broad standard described above.[38] However, only about 7 percent of those (barely more than 2 percent of the total submitted) supported an FBI investigation, led to one being opened, or involved a person on the terrorist watch list.[39] Worrisomely, SARs that are determined to have no connection to terrorism and are not uploaded to the ISE may still remain in a fusion center's files.[40]

DHS has never made public any assessment of fusion centers that meaningfully examines the quality of the information they report and attendant civil rights and civil liberties risks.[41] The most robust and methodical evaluation of fusion centers' intelligence reports was the Senate's 2012 report, which reviewed "every raw DHS intelligence report drafted on information from state and local fusion centers" over a 13-month period. It "identified problems with nearly every significant aspect of DHS's involvement with fusion centers" and offered scathing criticism of their efficacy and impact on civil liberties.[42]

Fusion center leaders have batted away questions about effectiveness, arguing that it is impossible to measure the centers' security benefits.[43] Despite fusion centers' questionable contributions to counterterrorism, their funding from combined federal, state, and local sources totaled some $336 million in 2018.[44]

Office of Intelligence and Analysis

The Office of Intelligence and Analysis serves as a conduit between federal agencies and their state and local partners for terrorism-related information.[45] In addition to supporting the national network of fusion centers, the office is authorized to carry out domestic surveillance — mostly limited to monitoring and acquiring publicly available information — in support of "authorized intelligence missions," including counterterrorism, threats to U.S. economic security or public health, and major disasters.[46]

Since the office collects and disseminates information about Americans, it must act with strict fealty to constitutional values and its specific security mission. But the guidelines that govern I&A are generally quite permissive. For example, the office is not allowed to undertake intelligence activities "for the *sole purpose* of monitoring" constitutionally or legally protected activities.[47] This is hardly an effective safeguard: it is easy to cite a pretextual but constitutionally neutral justification (e.g., an unsubstantiated contention that a protest could turn violent) to collect information on Americans' political organizing and religious practices.

I&A's activities in the summer of 2020, as racial justice demonstrations broke out across the country, illustrate how its institutional deficiencies open the door to abuse.[48] Pursuant to an executive order aimed at quelling protests under the guise of protecting federal buildings, the office issued guidance labeling "threats to damage or destroy any public monument, memorial, or statue" as justification for sweeping intelligence gathering.[49]

The disclosure of this guidance raised concerns in Congress. Rep. Adam Schiff (D-CA), chair of the House Permanent Select Committee on Intelligence, declared that "never before has the Department sought to so aggressively counter potential threats of graffiti, vandalism, or other minor damage . . . in the same fashion as it would seek to counter acknowledged threats . . . such as terrorism."[50] I&A's compilation and dissemination of intelligence reports summarizing tweets by two journalists about this guidance ultimately triggered an investigation by the department's inspector general and a review by its general counsel's office.[51] The latter, which was completed in January 2021 and made public in October of that year by Sen. Ron Wyden (D-OR), detailed failures of leadership, management, and rule compliance at I&A and raised questions about its overall value.[52]

While the general counsel's review did not find evidence of politicization per se, it showed that bias rather than facts drives DHS's intelligence priorities. For example, in keeping with the Trump administration's insistence that Antifa was behind racial justice protests, an unnamed senior I&A official pressured analysts to describe threats as "inspired" by "violent antifa anarchists."[53] The unit's acting chief during this time claimed in a whistleblower complaint that DHS leadership asked him to change various intelligence assessments to substantiate President Trump's public remarks, including on the supposed dangers posed by "ANTIFA and 'anarchist' groups" operating throughout the United States.[54]

The lack of adequate rules and safeguards makes DHS's intelligence arm a ripe target for manipulation. The general

counsel recommended a "holistic review of the strategic direction of I&A," including an evaluation of "buy-in" from various nonfederal governmental partners and the broader DHS intelligence enterprise, as well as of I&A's contributions to violence prevention and intelligence analysis.[55] The general counsel's review essentially called for an assessment of whether I&A is serving its statutorily designated role as a nerve center for intelligence sharing on threats within the United States. The review highlighted several systemic problem areas:

- **Poor training.** All I&A personnel collecting open-source information on "current and emerging threats" demonstrated "major gaps" in understanding the scope of collection "affecting First Amendment issues and the Intelligence Oversight guidelines."[56]

- **Difficulty of identifying threats of violence.** As the review noted, identifying real threats of violence "is a difficult task filled with ambiguity," and distinguishing between "serious threats and hyperbole" can be "subjective." It recommended that I&A's Current and Emerging Threats Center (CETC) shift its focus from immediate threats back to strategic intelligence collection and analysis.[57]

- **Insufficient safeguards for Americans' information.** According to the review, prior to the summer of 2018, CETC had a practice of replacing the names of U.S. citizens and lawful permanent residents with a generic marking (e.g., "U.S. person") in certain reports based on information collected from publicly available sources such as social media to minimize risks to privacy and to civil rights and civil liberties. The lack of a formal policy enabled the Trump administration to easily discard these rules, allowing sensitive "U.S. person" information to be freely disseminated.[58]

- **No plan to structure intelligence collection.** I&A's open-source analysts did not follow the standard intelligence community practice of starting information collection with a plan identifying the need it is meant to fill and how it will be collected. The review observed that having a plan in place reduces the potential for collection that is aimed at proving a foregone conclusion and helps build a "culture of compliance."[59]

Based on these findings, the general counsel's review recommended that DHS carry out an objective evaluation of I&A's strategy, structure, and counterterrorism value.

A March 2022 report by DHS's inspector general largely underscored the findings in the general counsel's report, portraying I&A's analysts as woefully undertrained and subject to political headwinds. The inspector general reviewed I&A's open-source intelligence collection in the weeks leading up to the January 6 attack on the U.S. Capitol.[60] In contrast to the 366 open-source intelligence reports that I&A issued during the racial justice protests that occurred between May 25 and August 24, 2020, it issued no reports in the weeks leading up to the January 6 attack, despite a direct request for research from I&A's unit responsible for producing finished intelligence.[61] I&A analysts claimed they viewed the threats of violence they identified online as "unlikely" to come to fruition, despite seeing calls to action by known violent actors such as the Proud Boys.[62] I&A officials also claimed that directions from the office's leadership changed between the two events, with analysts told to report "anything related to violence" during the 2020 protests but only to report threats "they were confident . . . were real" ahead of January 6.[63]

While the inspector general did not probe the nature of the changed perception of threats by collectors and instructions from superiors — focusing instead on the fact that most collectors received only minimal training and had less than one year of experience — it is difficult to avoid the conclusion that the race and political leanings of those planning the gatherings played a role.[64] In March 2022, Stephanie Dobitsch, the deputy undersecretary for I&A, testified to Congress that in response to its failures in the lead-up to January 6, I&A "has made substantial changes to the management, policies, equipment, personnel, organization, and training associated with our open source intelligence activities," improved the oversight over open-source reports, and doubled the staff for I&A's Privacy and Intelligence Oversight Office (though the absolute numbers are not publicly available), including dedicating an officer to the open-source team.[65]

It is difficult to gauge the extent to which these changes address the systemic and long-standing issues at I&A. Even before its activities drew sustained scrutiny, the office was issuing inappropriate intelligence reports. Although such reports are often quickly withdrawn after they become public, their issuance points to deep-seated institutional problems. For example, in 2007, the office issued a study on the Nation of Islam that was subsequently withdrawn because, as one senior official conceded, "the organization, despite its highly volatile and extreme rhetoric, has neither advocated violence nor engaged in violence."[66] In 2009, I&A published a report on right-wing extremism that was criticized by Republicans and Democrats alike in Congress for targeting nonviolent groups such as veterans and opponents of immigration and abortion.[67] DHS quickly withdrew the report and disbanded the small unit that produced it, which had been tasked with studying "non-Islamic extremism."[68] While the report may seem prescient in retrospect, it was filled with suppositions and cast various political views as threatening without demonstrating any connection to violence.[69]

More recently, I&A monitored Twitter for information about 2015 protests in Baltimore over the killing of Fred-

die Gray, a young Black man who died while in police custody; in searching social media, I&A overstepped its mandate by scrutinizing political dissent.[70] In 2017, the unit produced several reports on Antifa and "anarchist extremist" violence that were based primarily on information drawn from an unreliable far-right website.[71] And the next year, it reportedly disseminated information gathered from social media on hundreds of protests against the Trump administration's family separation policy to I&A staff, Immigration and Customs Enforcement (ICE) personnel, and state and local partners.[72]

Violence Prevention Programs and Partnerships

As part of its terrorism prevention mandate, DHS is charged with supporting and coordinating violence prevention efforts, which since 2021 have been undertaken by its Center for Prevention Programs and Partnerships (CP3).[73] A key goal of CP3 is to identify individuals who exhibit purported warning signs of violence for referral to law enforcement or to multidisciplinary teams that include law enforcement; these teams collectively determine whether the individual poses a threat and form an intervention plan to manage the ostensible risk.[74] CP3 is built on the discredited premise that commonplace feelings, views, and behaviors are predictive of an inclination to violence. As DHS acknowledges, law enforcement "cannot operate" the types of programs funded by CP3 "because of constitutionally based civil rights and liberties."[75] Nonetheless, CP3 provides opportunities for police to become involved in these programs.[76]

CP3 grew out of the Countering Violent Extremism (CVE) initiative, which formally became part of the U.S. counterterrorism strategy in 2011.[77] The scheme provided funding to police departments, academics, and civil society organizations to train teachers, social workers, and religious figures to identify American Muslims who might "radicalize" and become terrorists and to disrupt their progress toward violence. The Biden administration has rightfully recognized that CVE was a biased initiative.[78] Indeed, past CVE programs targeted Muslims almost exclusively and often relied on overtly prejudiced — and empirically unfounded — indicators, such as frequent attendance at a mosque or concerns about anti-Muslim discrimination.[79]

In 2019, CVE was renamed Targeted Violence and Terrorism Prevention and its focus broadened from political violence by Muslims to a wider spectrum of political violence, along with "targeted violence," an indeterminate category. In 2021, it was again rebranded, this time as CP3.[80]

There is simply no evidence to show that this strategy of preventing violence works. A RAND Corporation study that DHS has claimed validates its approach in fact undermines it: "Because there are no unambiguous early indicators of future violent behavior, the performance of risk assessment tools and methods to distinguish individuals who *appear to be threats* from those who *actually do pose a threat* is limited."[81]

This finding is hardly surprising. Millions of Americans share the conditions that DHS identifies as signs of impending violence, including "social alienation," having a "grievance," or "negative home life factors" (such as coming from a single-parent household). Even purportedly extreme views do not necessarily predict violence: while nearly all terrorists have "extreme" views, so too do millions of people who never plan or commit a violent act.[82]

CP3's aim to do away with the most blatantly biased aspect of CVE — its near-exclusive focus on Muslims — does nothing to prevent bias from creeping into programs. People tasked with being on the lookout for vaguely articulated suspicious behavior, such as "severe mood swings" or "feelings of hopelessness," are inevitably influenced by individual and societal prejudices.[83] Such biases and their attendant harms are well established; in schools, for example, students of color are punished more often and more severely than white students for the same behavior.[84]

Moreover, at a time when jurisdictions around the country are considering how to reduce law enforcement involvement in mental health and social issues, CP3 prevention activities take the opposite approach: they categorize a broad range of concerns about mental health and socioeconomic conditions as indicators of criminality and bring them to the attention of law enforcement.

Despite DHS's claims that these programs are successful, its own assessments have not demonstrated that they prevent violence.[85] Rather, the agency's evaluations rely on unrelated performance metrics, focusing instead on the reach of a program or the degree to which a grantee has fulfilled funding conditions, while simply presupposing that violence reduction will follow if the department's prevention framework is implemented.

A 2021 evaluation of a grant provided to Crisis Intervention of Houston illustrates the point. According to DHS, the purpose of the grant was to build up a hotline aimed at reducing extremism, including adding "a Muslim youth–oriented hotline." Success was defined via metrics such as increasing the number of counselors and outreach events aimed at the Muslim community.[86] But although a number of counselors were trained and outreach events held, none of the calls handled by the hotline seem to have related to violent extremism.

Despite the risks associated with the CP3 approach and a lack of evidence that it actually prevents violence, Congress continues to fund it, including by providing $20 million for CP3's Targeted Violence and Terrorism Prevention grant program in 2022.[87]

II. Data Collection, Risk Assessments, and Profiling

DHS collects reams of data about travelers; this data is stored in opaque, interlocking databases, powering secret risk assessments that shape each traveler's experience. The department's antidiscrimination policies are not up to the task of preventing bias in these activities, and travelers have repeatedly complained about profiling by DHS agents on the basis of religion, ethnicity, and national origin.

Data Collection

Much of DHS's power comes from the sheer amount of personal data it accumulates. As two former DHS officials have observed:

> [DHS] is the only government entity that, as part of its regular operations, conducts invasive physical searches of millions of Americans and their belongings each week without any predicate. It is also one of the only government agencies that retains huge amounts of data on individuals, using only "implied consent" for justification. In addition, it draws inferences based on data in ways that are totally opaque to citizens, and takes actions that may be to their individual detriment (being selected for search and interrogation, being delayed or severely inconvenienced in their travel, etc.). . . . [T]he privacy and due process concerns resulting from other homeland security operations, such as information collection by the National Security Agency, pale by comparison.[88]

In contrast to the NSA's data collection, which has been the subject of much congressional and public scrutiny, DHS's data programs often fly under the radar. Yet these programs give the department a deeply intimate view of many Americans' lives through a range of information, including the following:

- biometric data, including not just fingerprints and digitized photographs of foreign travelers but also facial recognition records for both foreign travelers and U.S. citizens;[89]
- social media information obtained from travelers' electronic devices or through vetting of travelers or their online contacts;
- information retrieved by border agents from travelers' phones, laptops, or other devices, including data obtained from social media apps, as well as notes about these encounters;[90]
- free text notes entered into DHS databases in the course of border crossings, which have contained information about First Amendment–protected activities, such as the books carried by travelers and the conferences they have attended;[91] and
- passenger name records, which generally include contact information, seat numbers (allowing inferences about travel companions), and credit card data, and which may even disclose IP addresses from which flight reservations were made and details about hotel reservations.[92]

DHS is increasingly buying information about Americans from commercial data brokers as well. In February 2020, the *Wall Street Journal* reported that DHS was purchasing GPS-based cell phone app location data from the commercial firm Venntel under contracts worth millions of dollars.[93] CBP, ICE, and the U.S. Secret Service also reportedly have contracts with Babel Street, a data analytics company, to identify devices in particular areas and build historical records of their prior locations.[94] The department has repeatedly refused to offer clarification about how it uses the data, however, and the DHS inspector general indicated in November 2020 that he intended to launch an investigation into the practice.[95]

Location is highly revealing, as the Supreme Court noted in a 2018 case concluding that police must get a warrant to access stored location data collected by cell phone providers.[96] The Internal Revenue Service inspector general issued a letter in 2021 indicating that purchasing such data may run afoul of that decision.[97] In the meantime, individuals may have minimal practical awareness that their location data is being sold to the government: apps' terms of service generally provide little notice that the data they gather may be funneled to the government through data brokers.[98] Data held by these companies is supposedly anonymized, but much of it can easily be de-anonymized and can be used to identify and track individuals based on their real-world behavior.[99] Location data can also be used to target communities that have historically been subjected to government monitoring. Researchers have revealed, for

example, that Muslim users are a "conspicuous target" of location surveillance through consumer apps — data that could then show up in commercial databases available for purchase by DHS.[100]

Data about people's identities and activities on social media is flowing into DHS databases in ever-increasing volumes as well. This collection effort began near the end of President Barack Obama's second term, when the department began asking for social media handles from approximately 15 million foreign travelers per year.[101] In 2019, the State Department started requiring an additional 14 million visa applicants annually to disclose their social media handles, which are shared with DHS and retained in its databases.[102] As the Biden administration reviews these programs, it should take into account not only the known risk of misinterpretation of social media content[103] but also the government's own findings:

- DHS has described social media handles as "sensitive personally identifiable information," which is information that "if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual."[104]
- DHS pilot programs found social media screening practically useless in support of adjudicating immigration benefits, with officers having difficulty using social media to pinpoint fraud or national security concerns.[105]
- A 2017 DHS inspector general report found that the department's failure to measure the effectiveness of social media monitoring during pilot programs gave it no basis for further efforts.[106]
- The Office of Information and Regulatory Affairs (OIRA), the White House office that reviews federal regulations, in April 2021 rejected a DHS proposal to collect social media identifiers from another 33 million people per year. OIRA noted in rejecting the proposed plan that the department had not "adequately demonstrated the practical utility of collecting this information," and that the Muslim ban, which underpinned the proposal, had been repealed.[107]

CBP and ICE also collect data through border searches of phones, laptops, tablets, and other electronic devices at land crossings and at airports for passengers arriving on international flights.[108] In fiscal year 2021, CBP conducted more than 37,000 searches of electronic devices; in 2018, when statistics about the citizenship of those targeted were last available, approximately 20 percent of such searches involved U.S. citizens.[109]

Guilt by Association

>> **In the summer of 2020,** Ismail Ajjawi, a Palestinian student from Lebanon, flew into Boston's Logan International Airport to start his first year at Harvard University. A CBP officer examined his phone and, according to Ajjawi, denied him entry because "she found people posting political points of view that oppose the U.S. on my friend list."[110] He was sent back to Lebanon and barred from reapplying for a U.S. visa. After intense media scrutiny and pressure from Harvard, Ajjawi was allowed to begin his studies in the United States. But few people denied visas or immigration benefits such as green cards or naturalization will ever know whether social media posts — their own or those of their online contacts — were to blame.

The system operates behind closed doors, allowing political, ideological, and religious vetting — not just of applicants but also of their online "friends" — to take place unchecked. Moreover, social media can easily reveal intimate aspects of people's lives, such as their sexuality, whether they own guns, their support for organizations like Planned Parenthood, or their mosque, synagogue, or church attendance. As Ajjawi's experience shows, social media monitoring can be used to target people whom the authorities disfavor by facilitating the ability to refuse them entry into the country, deport them, subject them to investigation, share their information with a repressive foreign government, or just hassle them at the airport.

Even though its data collection rules give it ample latitude, DHS has often failed to comply with them. According to a 2018 inspector general report, CBP agents regularly failed to properly document searches and to disable cell phone network connections prior to searches — requirements meant to restrict agents' access to information stored outside the device.[111] The report also found that CBP had no performance measures in place to assess the effectiveness of its forensic searches, including whether these searches resulted in prosecutions or convictions.[112] A September 2021 follow-up blasted CBP's progress since the previous report, disclosing failures in documentation, compliance, auditing, evaluation of efficacy, and training.[113]

Other flaws have plagued the department's use of electronic device searches as well. Journalists, activists, and Muslim travelers contend that they have been subjected to targeted device searches based on their activities or religious affiliations.[114] The section below describes the use of a DHS database to facilitate the search and seizure of an American traveler's electronic device based on his political activity.

Data Storage and Analysis

When data is collected, it needs someplace to go. DHS has no shortage of databases, some of which double as sophisticated analytical tools. One of the most high-profile databases to which DHS both contributes and has access is the Terrorist Screening Database (TSDB), an FBI-maintained watch list of people who are ostensibly known or suspected terrorists.[115] As of 2017, about 1.2 million people were on the watch list, including about 4,600 U.S. citizens.[116] The list, which includes individuals nominated by the FBI and DHS, has long been criticized for using vague criteria to identify individuals for additional scrutiny and for lacking a mechanism by which Americans can challenge their inclusion.[117]

Lesser-known data systems operating in the background also have a substantial impact on travelers' liberties, including those of U.S. citizens. Take, for example, the Automated Targeting System (ATS), which uses pattern-based algorithms to attempt to identify putatively threatening individuals.[118] ATS includes information compiled by airlines;[119] license plate and department of motor vehicles registration data; law enforcement, intelligence, visa, and immigration enforcement data; the TSDB and other watch lists; data accessed through border searches of electronic devices; commercial data; and more.[120]

Another CBP risk assessment platform, the Analytical Framework for Intelligence (AFI),[121] also draws from a vast array of data sources, including ATS; TECS, a system used both to store border-related data and to screen travelers to determine admissibility;[122] a variety of passenger data; and information from a now-defunct program that required primarily Arab men to register with the federal government.[123] Some AFI users can also upload and store social media data and other information from the open web.[124]

These massive systems operate without sufficient controls. CBP agents can access a range of sources — from biometric data to information retrieved from electronic devices, from law enforcement databases and commercial data provided through LexisNexis to records about travelers flying over the United States — simply to vet a traveler who is sent to secondary inspection, a step that does not require any suspicion of criminal activity or a threat.[125] And access is not limited to agents carrying out border security functions: in some circumstances, other DHS components that carry out intelligence functions can obtain data from the system.[126] Indeed, the controls are so weak that DHS cannot even guarantee that AFI users are authorized to access the data they retrieve.[127]

Challenging the Terrorist Screening Database

>> **Multiple court challenges** have been filed against the TSDB in recent years. Although the results in these cases have been mixed, the recurring litigation shows that these concerns are persistent and ongoing.

- In 2016, 25 American Muslims sued DHS and other federal counterterrorism agencies, claiming that they had been detained and harassed when entering the United States because of their presumed inclusion in the database.[128] A Virginia federal district court ruled in their favor in 2019, concluding that the vague standard for adding people to the watch list presented a high risk of "erroneous deprivation" of their protected liberty interest in travel and that the procedural safeguard provided — DHS's Traveler Redress Inquiry Program (TRIP) — was insufficient.[129] The decision was reversed on appeal on the grounds that the government has the authority to regulate travel and that only Congress or the White House can substantially alter the operation of the TSDB.[130]

- In 2020, 39 American Muslims filed suit in federal court in Maryland challenging several government watch lists, including the TSDB.[131] The court rejected the government's motion to dismiss the case, finding that the plaintiffs had a protected liberty interest in travel and that individuals who attempted to use TRIP could end up in a bureaucratic "black hole," stymieing their efforts to vindicate that interest. The judge allowed the case to proceed to discovery, which is ongoing.[132]

- A 2021 case filed by the American Civil Liberties Union on behalf of a U.S. citizen alleging that he had been wrongly placed on the so-called No Fly List, a subset of the TSDB, after he refused to become an FBI informant was withdrawn when the FBI removed him from the list shortly after he filed suit.[133]

The wide-ranging functionalities of DHS data systems lend themselves to abuse. DHS data architecture was used, for example, to target David House, a computer programmer who set up a website for U.S. Army whistleblower Chelsea Manning that included a petition for her release and an effort to raise legal funds. In 2010, House was stopped at the border and interrogated about his political activities and beliefs; his laptop and other devices were seized for copying and data analysis.[134] A settlement

revealed that ICE agents had used TECS and the Advance Passenger Information System to receive automatic alerts about House's travels in and out of the country, enabling investigators to stop and question him and seize his data.[135] House was never charged with a crime.

CBP also used TECS to target and harass journalists, attorneys, and activists — including 15 U.S. citizens — for their association with the caravan of migrants and asylum seekers arriving at the border with Mexico in 2018 and 2019. A September 2021 OIG report revealed that nearly half of the people flagged by these TECS lookouts were not suspected of any criminal activity; in one case, a lookout was placed on an individual whose only connection to the caravan was having crossed the border with one of its apparent organizers months earlier.[136]

This absence of any policy meaningfully limiting the use of DHS's powerful data systems undergirded an even more shocking story. In late 2021, Yahoo News reported that agents at CBP's secretive Counter Network Division regularly used highly sensitive databases to obtain travel records and financial and personal information about "journalists, government officials, congressional members and their staff, NGO workers and others," in order to vet potential contacts.[137] A former CBP agent told Yahoo, "there's no policy and procedure," confiding that he vetted reporters and others using TECS, ATS, and other databases as though they were terrorists, despite the absence of any evidence of criminal activity.[138]

Long retention periods and expansive sharing authorities magnify opportunities for misuse.[139] For instance, Silent Partner and Quiet Skies, two TSA risk assessment programs described in more detail below, have a retention range of 15 and 7 years, respectively;[140] TSA watch list master files are kept for 30 years after an individual's information is entered,[141] and TECS subject records and inspection reports are kept for up to 75 years.[142] Several of these data sets can be used for risk assessments during the entire retention period, and some systems even retain data after it has been deleted from the source system.[143] The nearly indiscriminate ingestion and long-term retention of data mean that mistakes can proliferate across systems.

In addition, the department's assertions of the efficacy and necessity of these systems are of dubious credibility at best. With respect to ATS, for instance, DHS has not conducted any public empirical evaluations of the system's effectiveness or weighed the benefits of its risk assessments against the dangers of collecting oceans of data about people, the vast majority of whom are innocent of any crime. A 2019 report highlighted two cases in which CBP officers used the system to identify one departing passenger who was wanted for child sexual assault and another, deemed a high risk for fraud, who turned out to be in possession of a fake passport.[144] ATS's predictive systems do not seem to have played much of a role in identifying the child abuse perpetrator; he had already been identified by another system, and all that was left was to apprehend him. ATS did assist in identifying the perpetrator in the fraudulent passport case, but if these are the best cases that DHS can highlight for a given period, they hardly seem to justify the entire ATS architecture.

Trapped by a Typo

>> **In 2005, Rahinah Ibrahim,** a Malaysian doctoral student studying architecture at Stanford University, was placed under arrest at San Francisco International Airport while en route to a conference in Hawaii. After being handcuffed and interrogated, she was told that her name appeared on the No Fly List but would be removed. She then continued on her journey and flew home from Hawaii to Malaysia. Ten weeks later, as Ibrahim sought to fly back to the United States, the airline informed her that her U.S. visa had been revoked. She filed a complaint with DHS to remove her name from the list but received no response.[145]

Ibrahim filed a lawsuit against DHS and other government agencies to remove her name from the No Fly List and other terrorism databases. In the course of the eight-year-long court battle that followed — during which time Ibrahim continued to be barred from the United States — an FBI agent admitted to accidentally placing a check mark on a form, resulting in the "considerable consequence" of her name being added to the list. Ibrahim's daughter was also mistakenly added to the No Fly List, preventing her from testifying at the trial. The court ultimately ordered the government to search for and remove references identifying Ibrahim in all of its terrorist watch lists and records, as well as to provide Ibrahim with information specifying why her visa had been revoked. In light of its years-long pursuit of the case, during which it knew Ibrahim posed no threat, the government was ordered to pay most of the nearly $4 million her legal team expended on her behalf.[146]

Other DHS data systems, such as the new Homeland Advanced Recognition Technology (HART) database, raise additional concerns. That system, which does not yet have a comprehensive set of public documents disclosing its scope, operations, or privacy mitigation measures, combines biometric data, data from social media platforms, and information from other publicly available online sources to facilitate analysis of relationship patterns. HART has been criticized on the grounds that it could be used for wholesale tracking and that it will combine massive quantities of disparate data sources in one place, creating a broad picture of an individual's life and relationships and implicating First Amendment concerns.[147]

These problems would be significant enough if DHS were transparent about the parameters of its information systems, enabling the public to understand what information is being amassed about them and what happens to it. Instead, as discussed below, the documentation produced by the DHS Privacy Office about the department's various databases, although voluminous, is often impenetrable to the lay reader. Even for experts, it generally only offers fragmented insight into how the department collects, uses, and shares individuals' data.[148]

Risk Assessments

DHS's collection and storage of data provides the raw material for its risk assessments, which are generated in part by closely held algorithms. CBP and TSA run risk assessments on every traveler, including U.S. citizens, arriving in and departing from the United States as well as those flying over domestic airspace on any airline or flying internationally on U.S. carriers.[149]

Some risk assessment programs have garnered sporadic congressional and media scrutiny, but they have at most been modestly curbed to mitigate their most intrusive aspects; the programs themselves remain a key part of how DHS currently implements its mission. These programs represent an extraordinary exercise of unchecked authority coupled with lackluster efforts to measure their effectiveness. Two programs about which ample public information is available are highlighted below. Others operate in the background with unknown parameters and consequences.

Screening of Passengers by Observation Techniques

Since 2003, TSA has sought to identify potentially risky passengers at airports through a program targeting purportedly suspicious behaviors such as wearing "improper attire for the location," gazing downward, and giving "nonanswers" to security personnel.[150]

The Extreme Vetting Initiative

>> **The danger that risk assessment programs** can be manipulated and even weaponized was underscored by a program that ICE began pursuing shortly after President Trump's inauguration: the Extreme Vetting Initiative. In the summer of 2017, ICE sought to find out whether private firms could build a tool to monitor Facebook, Twitter, and the rest of the open internet to automatically flag people for deportation or visa denial.[151] Trump's January 2017 executive order creating the discriminatory Muslim travel ban provided the basis for the nebulous screening criteria, which included whether the individual would be a "positively contributing member of society" and "make contributions to the national interest," as well as whether they would be likely to commit a crime or terrorist act. The contractor supplying the tool would have been required to flag at least 10,000 people each year for either deportation investigations or visa denial.[152]

As more than 50 civil society organizations told DHS, the program was "tailor-made for discrimination" and would have chilled the free expression of targeted individuals, along with their families and associates.[153] It also had no empirical basis: according to a letter to DHS signed by 54 leading experts in machine learning and automated decision-making, there are "no computational methods" that can predict whether a visitor or immigrant poses a risk or will contribute to society.[154] In the face of pressure, ICE dropped the automated aspect of the program, hiring human reviewers instead.[155] Little public information is available about this manual program, which was rebranded as the Visa Lifecycle Vetting Initiative.[156]

The initiative, called Screening of Passengers by Observation Techniques (SPOT) at its inception, deployed more than 3,000 behavior detection officers at airports around the country to look for these behaviors, identify passengers for additional screening, and identify trends.[157]

Governmental bodies have repeatedly questioned the scientific validity and effectiveness of SPOT, which cost $1.5 billion over about eight years.[158] The program has also been dogged by allegations that officers disproportionately targeted Black, Latino, and Muslim travelers. A stream of assessments from 2010 through 2017 all concluded that TSA was sinking hundreds of millions of dollars into a program with no proof that it contributed to public safety — and no plan to produce such proof:

- **2010.** A study by the U.S. Government Accountability Office (GAO) found that DHS had deployed the program without validating its premise and observed that there was no scientific consensus "on whether

behavior detection principles can be reliably used for counterterrorism purposes."[159]

- **2013.** An audit of the program by the DHS inspector general found that TSA could not "ensure that passengers at U.S. airports are screened objectively, show that the program is cost-effective, or reasonably justify the program's expansion."[160] A GAO report the same year urged that funding for the program be restricted until TSA could produce scientifically valid evidence supporting the use of behavioral indicators for risk assessment.[161]

- **2016.** A follow-up OIG report found that while the agency had implemented some performance metrics, it still had not determined the effectiveness of the program, rebranded by that point as Behavior Detection and Analysis.[162]

- **2017.** The GAO reported to the House Committee on Homeland Security that TSA "does not have valid evidence" that most of its indicators would actually help identify people who pose a threat.[163]

Unsurprisingly, the program — with its vague criteria and lack of scientific basis — resulted in profiling. According to a 2012 exposé in the *New York Times*, "more than 30 [SPOT officers] . . . say the operation has become a magnet for racial profiling, targeting not only Middle Easterners but also blacks, Hispanics, and other minorities."[164] At Boston's Logan International Airport, officers charged that "passengers who fit certain profiles — Hispanics traveling to Miami, for instance, or blacks wearing baseball caps backward — are much more likely to be stopped, searched and questioned for 'suspicious' behavior." One officer described the initiative in an anonymous complaint to TSA as "no longer a behavior-based program, but . . . a racial profiling program." Similar complaints surfaced about SPOT's implementation at the Newark and Honolulu airports.[165] And an April 2019 GAO report observed that while TSA policies prohibited profiling, there was no mechanism built into the program to monitor for possible violations.[166]

Although SPOT no longer operates as a stand-alone program, TSA agents evidently continue to be trained in and use behavior detection techniques.[167] Moreover, despite the serious concerns about the program's validity, SPOT records were approved by the department's Privacy Office to be kept for years or even decades and to be shared both inside DHS and with local law enforcement agencies.[168]

Secure Flight: Quiet Skies and Silent Partner

In August 2018, the *Boston Globe* disclosed another questionable TSA program, Quiet Skies. That program and a companion program, Silent Partner, were created in the wake of the attempted underwear bombing in 2009. The programs, which operate under the aegis of TSA's Secure Flight traveler vetting process, were hidden from view for nearly a decade after their inception.[169] Silent Partner reviews information about passengers on international flights bound for the United States, while Quiet Skies flags a portion of those inbound passengers for continued scrutiny during subsequent domestic U.S. flights and outbound international flights.[170] These individuals are targeted based on a set of evolving, nonpublic rules developed by TSA personnel and fed into ATS.[171]

Under Quiet Skies, armed federal air marshals boarded the flights of flagged passengers and noted whether they exhibited supposedly suspicious behaviors such as fidgeting, sweating, using the bathroom, conversing with fellow passengers, and staring. Flagged passengers were also subjected to extra screening upon arrival.[172] TSA officials reportedly told congressional staff that 5,000 U.S. citizens were monitored under this program between March and August 2018 alone, with none ultimately deemed suspicious or requiring further scrutiny.[173]

In a November 2020 audit, the DHS inspector general issued a blistering rebuke, determining that "TSA did not properly plan, implement, and manage" the Quiet Skies program.[174] As with other DHS surveillance programs, the audit found that the agency had failed to "develop performance goals and measures to demonstrate program effectiveness." Although TSA stopped requiring air marshals to report on the minutiae of their subjects' behavior after pushback from the public and from elected officials, marshals continue to surveil travelers — including those not suspected of criminal activity — and to document if their subjects do anything deemed suspicious.[175]

Religious and National Origin Profiling

DHS issued a policy in 2013 setting out the agency's "commitment to nondiscriminatory law enforcement and screening activities."[176] The document, which builds on the department's 2004 statement on racial neutrality and the Department of Justice's 2003 guidance on racial profiling in federal law enforcement, contains several loopholes and lacks a mechanism to fully vindicate its protections.[177] A stand-alone policy issued by CBP in 2020 is also beset by grave weaknesses.[178]

The strongest prohibitions in the DHS-wide policy are reserved for targeting on the basis of race or ethnicity, which is forbidden outside of the "most exceptional" cases; its use is permitted only when narrowly tailored to meet a compelling government interest.[179] This standard corresponds to constitutional protections and should bar practically all invidious uses of race or ethnicity if faithfully applied.[180] The department's policy further declares that it

is "erroneous" to assume that "any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity."[181] Of course, the same reasoning applies to an individual's faith, but DHS's nondiscrimination limitations are silent on targeting on the basis of religion.[182]

The absence of protections for religion has been keenly felt by Muslim American travelers, who have for years reported being singled out for questions about their religious views and national origin when traveling to or within the United States, including queries about what mosque they attend, how many times a day they pray, and what Muslim charities they support.[183] A heavily redacted sample questionnaire used by ICE has several questions clearly focused on Muslims, including "Do you have any relatives or friends who have been martyred fighting in the defense of your beliefs?" and "What is/are the name(s) of the martyr(s)?"[184] While religion may be relevant to decisions made by department personnel in certain narrow circumstances — generally only when it is explicitly required by law, such as when adjudicating a refugee or asylum application or an application for a religious worker visa — its untrammeled use in other contexts is unsupportable.[185]

The department also allows for the use of both nationality (citizenship) and national origin (country of birth) "based on an assessment of intelligence and risk," in situations in which "alternatives do not meet security needs," and for "only as long as necessary."[186]

For example, nationality can be used to make risk assessments, as discussed above. It may also be used when it is "expressly relevant" to administering laws related to a range of DHS functions.[187] Because many immigration and customs laws do require establishing a person's nationality (the visa waiver program, for instance, applies to citizens of 40 countries), some authorization to consider it is logical. However, nationality and national origin can also serve as a proxy for race, ethnicity, or religion. For example, President Trump's Muslim travel ban was formally based on nationality, as was President George W. Bush's program requiring boys and men from predominantly Arab and Muslim countries to register with the U.S. government.[188] Further, DHS policy permits the "individualized discretionary use" of nationality for screening, investigation, and enforcement, which gives the green light to arbitrary and biased targeting at airports and elsewhere.[189]

In January 2020, the *New York Times* reported that more than 60 Iranian American travelers had been held for questioning about their "political views and allegiances" at a border crossing between Canada and Washington State.[190] It was later reported that CBP's Seattle field office had instructed its agents to conduct additional vetting on individuals who were born in, traveled to, or held citizenship in Iran, Lebanon, or Palestine — that is, based on individuals' national origin and/or nationality.[191] The episode triggered congressional demands for information and a complaint to the DHS Office for Civil Rights and Civil Liberties; while the office did commence an investigation, there has been no news of its progress, despite repeated requests from members of Congress.[192]

The incident highlighted the susceptibility of departmental policies on nondiscrimination to abuse, in light of both their actual and implied permissiveness with respect to use of nationality and their ambiguity with respect to use of national origin. CBP's policy in particular emphasizes that it "does not in any way limit the individualized discretionary use of nationality" as a factor in screening, investigations, and enforcement, deeming the use of nationality to be "appropriate for the vast majority of situations encountered by frontline CBP personnel."[193] While the incident at the northern border instead involved a categorical instruction from a CBP field office, the highly permissive language in departmental policies is an invitation to push the boundaries and engage in discretionary targeting and screening more broadly.

The incident also underscored the tension between CBP's policy, which is entirely silent on national origin, and DHS's master policy, which at least purports to limit the use of national origin to "situations in which such consideration is based on an assessment of intelligence and risk" where there are no adequate alternatives, and only for as long as necessary.[194] The gap between the two policies may have signaled to CBP leadership that the discretionary use of national origin, even in the absence of reliable intelligence, would be tolerated or even tacitly permitted.[195]

Finally, DHS policy instructs components to ensure that officials are "held accountable" for following it, but contains no mechanism to proactively identify and address systemic issues of disparate treatment across the range of department programs and policies.

III. Oversight

Given the breadth of DHS's programs and their daily impact on Americans' civil rights and civil liberties, robust oversight is critical. It is sorely lacking. The weakness of the department's congressional oversight, which is spread across more than 100 committees and subcommittees that claim jurisdiction, has long been recognized.[196] This report focuses on the record of the three primary DHS-wide internal oversight mechanisms: the Office for Civil Rights and Civil Liberties, the Privacy Office, and the Office of Inspector General.

The first two offices suffer from structural weaknesses and have too often taken — or been pressured to take — a cramped view of their mandate, providing only limited transparency and oversight over the department's activities. OIG, which enjoys more independence than the other two offices, has provided greater transparency into the programs it audits and insisted on evaluations of their efficacy, but it has not paid sufficient attention to the repercussions for DHS programs on Americans' constitutional rights.

The shortcomings of the department's internal oversight structure have not gone unnoticed in Congress. In 2020, the House Homeland Security Committee chair, Rep. Bennie Thompson (D-MS), introduced a bill that would have strengthened CRCL and the Privacy Office and increased OIG's transparency.[197] The following year, the committee marked up bills to strengthen CRCL and increase disclosures by OIG.[198] Additional evidence of concern may be found in Congress's decision, during the Obama and Trump administrations, to appropriate significantly more funds for CRCL than the department requested.[199] These appropriations reflect lawmakers' recognition of the importance of improved oversight and protection of civil rights and civil liberties.

Office for Civil Rights and Civil Liberties

CRCL is charged with ensuring that DHS programs and activities respect the civil rights and civil liberties of those affected by them.[200] The office, which is headed by a non-Senate-confirmed presidential appointee who reports directly to the secretary of homeland security, plays three major roles:

- advising the secretary on the development, implementation, and review of DHS policies and procedures;[201]
- reviewing and assessing information about civil rights and civil liberties abuses, as well as racial, ethnic, or religious profiling by DHS employees and officials, and coordinating with OIG to investigate complaints;[202] and
- providing transparency by reporting to Congress, disseminating information to the public, and conducting outreach to a broad array of stakeholders.[203]

CRCL has not, however, served as an effective check on the department's powerful operational units. Although the secretary is charged with ensuring that the head of the office is advised of proposed policy changes and consulted by decision-makers,[204] a lack of access and influence appear to hamper the unit. Moreover, its dual role as internal adviser and guardian of constitutional values has created conflicts, with the office at times yielding to operational concerns. Unlike the Privacy Office, CRCL does not have the authority to issue subpoenas, making its information requests relatively toothless.[205] And its reports to Congress — which must be cleared by DHS leadership — provide such minimal detail about its activities that they do little to help the public understand the office's efforts.

Internal Counseling and Review

Much of CRCL's internal counseling role is hidden from public view, but people familiar with its operations have indicated that the office has had only limited influence. According to Scott Shuchart, who served as senior adviser to the CRCL officer from 2010 to 2018, the office "played a significant behind-the-scenes role in immigration enforcement and detention reforms" but was frequently left "in the dark until an action [had] progressed too far to be brought into compliance with civil rights and civil liberties requirements."[206] As a result, the office was unable to influence policy on a number of serious issues.

Similarly, Stanford University law professor Shirin Sinnar's 2015 study of the office found that it was widely regarded as ineffectual during both the Bush and Obama administrations.[207] Former Obama-era CRCL

officials told Sinnar that large and influential DHS components such as CBP and ICE "ignored CRCL policy recommendations and stalled in responding to complaints against those agencies." One former staffer described the office "as having 'zero influence' over most of the policy areas in which it engaged."[208] Similar reports emerged from staff who served during the Trump administration.[209]

Margo Schlanger, who led the office from 2010 to 2012, had a more sanguine assessment, highlighting instances in which the office influenced decision-making through direct input as well as by raising awareness of civil rights and civil liberties concerns within the department.[210] But civil society organizations and other stakeholders have often perceived the office as failing to fulfill its mandate.[211] Even Thompson, the House Homeland Security Committee chair, observed that CRCL had historically been "an afterthought," and DHS's own deputy secretary has spoken disparagingly of its influence.[212]

Part of CRCL's lack of clout may be attributable to the failure of departmental leadership to prioritize its mandate, but structural factors also play a role. CRCL has almost no formal review and consultation role, so it can simply be excluded from decision-making. Indeed, Thompson described it over a decade ago as being largely reactive to DHS policies implemented without its input, and the situation does not appear to have changed substantially since then.[213] This impotence was recently illustrated when the office was effectively sidelined as the Trump administration implemented its family separation policy at the U.S. border with Mexico.[214]

Moreover, CRCL seems to have little to no insight into or authority over many of the public safety and counterterrorism activities undertaken by DHS components. For example, some components have issued bulletins treating First Amendment–protected activities as threats, sometimes under the guise of "situational awareness."[215] Of course, these agencies need to understand the potential for major disturbances when planning for events, but they have often exceeded that mandate and cast even nonviolent protests as dangerous, as cataloged below:

- Under the guise of situational awareness, the Federal Protective Service issued a "civil activists and extremist action calendar" in 2006 listing advocacy groups and events gleaned from the internet. Of the 75 protests listed in the bulletin, at least 60 had no relation to the federal buildings or property that the service is meant to protect.[216]

- In 2015, the DHS Office of Operations Coordination (OPS) collected information on Black Lives Matter activities from public social media, including Facebook and Twitter, and Federal Emergency Management Agency watch centers likewise gathered information on police brutality protests in Baltimore and Philadelphia.[217] Around the same time, an unspecified DHS component was reported to be monitoring a prominent racial justice activist from Baltimore on social media.[218]

- New York City ICE agents used Facebook in 2018 to monitor anti-Trump protests, keeping a spreadsheet of left-wing groups, their goals, and the names of people who had signed up to participate.[219]

- Between 2016 and 2020, ICE regularly used social media and other means to monitor and intimidate immigrants' rights groups, activists, and journalists covering these issues. Agents tracked a candlelight vigil for a man who died in custody, preparing a "significant incident report" for a nonviolent event involving 19 people.[220] They also monitored the Twitter feed of a senior employee of the activist group Project South and tried to get her to remove posts about hunger strikes at a detention center.[221] During this four-year period, NYU School of Law's Immigrant Rights Clinic documented more than 1,000 cases of alleged retaliation by DHS against immigrant activists, including 318 perpetrated by ICE.[222]

When CRCL is given meaningful opportunity to provide input, it can serve a useful role. After the DHS Office of Intelligence and Analysis published its 2009 intelligence bulletin on right-wing extremism over CRCL's objections, creating a firestorm of criticism, CRCL was authorized to review I&A's finished intelligence products,[223] ushering in a period of fewer public controversies. In 2015, however, the press reported on I&A monitoring of protests in the wake of the fatal police shooting of Michael Brown and the death of Freddie Gray in police custody. The media attention prompted DHS to further strengthen and elaborate CRCL's role vis-à-vis I&A.[224] But with this role enshrined only in internal rules, the office was easily marginalized by the Trump administration, likely enabling I&A's participation in monitoring and suppressing racial justice protests in 2020.[225]

Impact Assessments and Complaints

Although CRCL has not published many of its reviews of alleged civil rights and civil liberties abuses, some information on its impact assessments and complaints is publicly available.

Impact Assessments

Impact assessments are program reviews that can cover "all types of policy, policy implementation, and practices," providing a critical opportunity for the office to make its

voice heard.[226] The DHS website lists eight CRCL impact assessments, all of them published prior to 2013.[227] The American Civil Liberties Union obtained an additional assessment produced in 2009.[228] There may be others that are not public.

The small number of published impact assessments and their apparent absence over the past nine years — a period in which the department launched numerous programs with the potential to undermine Americans' civil rights and civil liberties — suggests that the office has been missing in action.[229]

The publicly available impact assessments suggest that despite a statutory mandate to balance the need for a particular governmental power against protections for privacy and civil liberties, CRCL has often taken a perfunctory approach to analyzing a given program's security benefits as well as its impact on civil rights and civil liberties.[230] Three examples illustrate CRCL's evident reluctance to use its assessments as an opportunity to advocate forcefully for civil rights and civil liberties protections.

First, CRCL's 2009 impact assessment of the TSA SPOT program accepted without examination the "scientific behavioral research" on which the program was based.[231] By contrast, the 2013 analysis of the same program by the GAO — one in a series of critical reports described above — observed that "decades of peer-reviewed, published research . . . draw into question the scientific underpinnings of TSA's behavior detection activities."[232] On the issue of racial, religious, and ethnic profiling by officers deployed under SPOT, CRCL further failed to sufficiently address concerns about the broad discretion the program gave to officers. Instead, CRCL summarily concluded that officers were unlikely to engage in such misdeeds. Less than three years after the program launched, frontline officers came forward to report that such profiling was common.[233]

Second, CRCL's 2011 impact assessment of airport searches of laptops and electronic devices generally acceded to CBP's view that the searches did not require individualized suspicion despite their extreme intrusiveness, including their potential to reveal intimate details of their subjects' lives extending back years.[234] The office's legal analysis is entirely redacted in the public report, but it seems that CRCL was influenced by CBP's stated operational imperatives. A cautious approach by CRCL on legal issues that were not resolved at the time the assessment was completed may be understandable.[235] However, the office also found that requiring individual suspicion could be "operationally harmful without concomitant civil rights/civil liberties benefits."[236] As Sinnar pointed out, CRCL accepted the stated harm to operations "without any independent analysis of the claimed security need for suspicionless searches."[237] It is difficult to see how the office could fail to recognize the harms of invasive electronic searches and the litany of transgressions discussed in this report.[238]

Third, in sharp contrast to the Senate's highly critical 2012 report, CRCL's 2013 evaluation of fusion centers barely considered their effectiveness at identifying security threats and indicated that it was unaware of civil rights and civil liberties violations.[239] The office did make important recommendations, including that fusion centers focus on information supported by a reasonable suspicion of criminal activity (pursuant to 28 C.F.R. Part 23) and that DHS tighten protections for civil rights and liberties.[240] But, as discussed above, these recommendations have either been ignored or implemented perfunctorily.

Complaints

CRCL is charged with investigating complaints alleging civil rights and civil liberties abuses by DHS employees, though the inspector general has the right of first refusal.[241] For those that remain in CRCL's hands, CRCL may either investigate them directly or refer them to the relevant component and then review the component's findings.[242] While CRCL cannot provide complainants with a concrete remedy, it can advise DHS leadership to change the relevant policies.[243]

The number of CRCL complaint investigations doubled between 2014 and 2020, rising from 417 to 881, with the bulk relating to immigration and detention.[244] The office's most recent annual report to Congress indicated that it has also opened multiple investigations regarding "allegations about inappropriate questions into religious affiliation and practices at U.S. ports of entry." The office reported that CBP has "substantially improved officer training" and issued two recommendations to assist CBP in its "efforts to avoid improper questions regarding travelers' religion while conducting border inspections."[245] While these seem like positive developments, the vagueness of the information provided makes it difficult to gauge their efficacy. Indeed, an earlier recommendation from CRCL that CBP and ICE state in their policies that it is generally impermissible to discriminate against travelers on the basis of religion has not been adequately addressed.[246]

Transparency

Although the Homeland Security Act of 2002 requires CRCL to convey information to the public, its reports — submitted semiannually to Congress and to the independent Privacy and Civil Liberties Oversight Board — often fail to provide enough information to assess its work.[247] These reports tend to identify issues and programs on which the office has worked and indicate whether it made recommendations to the relevant DHS component. But they provide only bare-bones information on the nature of the problems or the recommendations made and do not typically reveal whether the component agreed to the recommended changes or report on their implementation. Former high-level DHS officials have suggested that

the process for clearing CRCL reports through the secretary of homeland security and the White House is responsible for deficiencies in them — for example, a lack of transparency about when advice has been "disregarded or excluded from policy development."[248]

Recently, the office has started publicly releasing some of the memorandums it issues to components on its investigations.[249] While redactions and the lack of detail about components' responses limit the usefulness of these disclosures, they do provide additional information about the types of complaints that CRCL is fielding.[250] Still, it is hard to come by more than a fragmented understanding of the office's contribution to protecting civil rights and civil liberties.

In sum, the concept of a civil rights and civil liberties watchdog within DHS has promise, but CRCL lacks the institutional support, the concrete authority, and, at times, the initiative to serve as a meaningful check on departmental overreach.

Privacy Office

Under its enabling statute, the Privacy Office is afforded broad powers. The chief privacy officer, who is appointed by the secretary, is directed to "assur[e] that the use of technologies sustain, and do not erode" privacy protections for personal information, and to undertake any "investigations and reports relating to the administration of the programs and operations of the Department."[251] Yet in practice, much like CRCL, the Privacy Office has not come close to fully exercising — or being supported in its exercise of — this authority.

Many of the office's public disclosures come in the form of privacy impact assessments (PIAs). These documents focus on detailing the privacy implications of various DHS data collection systems and programs and explaining how privacy concerns are mitigated, often via procedural and technical means. Because PIAs address individual data systems, they represent a siloed approach that makes it difficult to understand the interconnected operations of the department's vast and ever-growing holdings, which numbered more than 2,000 data sets as of May 2021.[252] Notably, the chief privacy officer — who has broad statutory authority to undertake investigations of "possible violations or abuse" in any DHS program as well as the authority to subpoena documents and testimony[253] — has conducted only one public investigation, now a decade past, even as DHS has acquired and deployed myriad new systems for collecting information about Americans.[254]

Adding to these problems, a 2020 OIG report concluded that the Privacy Office did not have "effective oversight of department-wide privacy activities, programs, and initiatives."[255] According to the report, the office had not exercised adequate oversight over agreements covering the disclosure of information from DHS to other federal agencies and third parties. Even with respect to reviewing compliance documents, the office was years behind schedule. And it had not monitored whether personnel were completing required privacy training; the OIG's investigation revealed that approximately half of all headquarters staff — nearly 5,000 people — had failed to complete training over a two-year period.[256]

Structural Advantages

Compared with CRCL, the Privacy Office enjoys several structural advantages that give it better access to information and influence, and it also benefits from greater protections from both internal and external interference. Each DHS component is required to have its own privacy officer, who performs oversight activities in coordination with the chief privacy officer;[257] the chief privacy officer in turn is positioned to provide headquarters privacy staff with insight into operational developments at the component level. The requirements for oversight and compliance documentation, such as PIAs, also give the Privacy Office specific points of leverage. Finally, the chief privacy officer oversees the submission of multiple mandated reports to Congress and the public.[258]

Under a 2007 law, in addition to reporting to the secretary, the chief privacy officer submits annual congressional reports that are statutorily protected from internal and external interference, conferring additional authority and insulation.[259] In short, unlike CRCL, the Privacy Office cannot simply be ignored or kept out of the loop — though the fact that the officer is appointed by the secretary rather than the president has tended to weaken the office's authority within the department.

Privacy Mandate Implementation

Despite these advantages, the office has often fallen short of fulfilling its transparency and oversight mission. The compliance documents for which it is responsible sometimes give short shrift to privacy concerns, and they rarely provide sufficient information to allow for a public understanding of the complex data systems on which DHS relies.

Under the Privacy Act of 1974 — a measure passed in the wake of Watergate — DHS components are required under certain circumstances to publish a system of records notice (SORN) in the *Federal Register*.[260] SORNs, which cover government databases from which personal information can be retrieved by an identifier, such as a name or social security number, alert the public when a government agency creates a new covered database or updates an existing one; the Privacy Act gives individuals whose data is included in a covered system the right to request their records, to change inaccurate, irrelevant, or

incomplete records, and to be protected against invasions of privacy based on the collection, maintenance, use, and disclosure of their data. But records systems implicating law enforcement and national security are exempt from a number of the Privacy Act's provisions, and DHS's SORNs frequently set out extensive exceptions to the act's requirements on those grounds.[261]

The Privacy Office seems to place a sizable portion of its resources into PIAs, which are meant to cover "what information is collected and why; how the information will be used, stored, shared, and accessed; how the information will be protected from unauthorized use or disclosure; and how long the information will be retained."[262] While PIAs check these boxes, they often make only a modest contribution to informing the public about the privacy impact of DHS's activities or how their data might actually be collected and used. In addition, because each PIA only covers a particular system or program, they fail to tell the whole story of how DHS ingests and internally shares data arising from interactions across multiple agency systems.

For example, travelers who visit the United States under the program for visa-free travel and fill out an online application through the Electronic System for Travel Authorization (ESTA) would first need to review the ESTA PIA to understand how their information is being processed. Then they would have to review the PIAs of all the other databases that are checked as part of ESTA processing.[263] Upon arrival in the United States, the travelers would also be subject to DHS's biometric entry and exit program, which implicates yet another PIA.[264] Even if they could understand each individual document, they would not be able to discern the interaction between the range of databases and screening tools that affect them.

In short, there is no top-down picture of the full scope of DHS's data holdings. PIAs, SORNs, and related documents offer only a tunnel view of how a particular type of data might be used, with whom it might be shared, and how long it might be retained. The public has no real way to fully grasp the department's data management.

Such data fragmentation is not inevitable. The department's annual data mining reports, for example, typically offer a broader view of the impact of covered operations than PIAs, including more user-friendly descriptions. However, these reports are required only for programs involving data analysis aimed at uncovering patterns that ostensibly predict terrorist or criminal activity. No analogous requirement exists for a data system or analysis tool that simply collects, uses, or extracts information about a particular individual or group.[265]

The final piece of the privacy oversight structure is the privacy compliance review (PCR), which assesses programs' fidelity to privacy rules, including assurances made in PIAs, SORNs, and information-sharing agreements.[266] If the Privacy Office uncovers "potentially egregious behavior" during a review, it will refer the matter to the inspector general or open an investigation itself.[267]

In November 2020, the Privacy Office analyzed 20 open PCR recommendations and published a report revealing significant delays in the implementation of certain privacy mechanisms. In 2015, for instance, the office recommended that a 2013 directive on CBP's use of passenger name records be "promptly updated." Five and a half years later, the updates were still "ongoing" and the 2013 directive — at that point more than seven years old — was still in place.[268] In 2017, the office recommended that OPS "fully implement" the DHS requirement that it have its own privacy officer. Three years later, Privacy and OPS were still "continu[ing] to discuss" how to implement that DHS policy rule.

Perhaps the most notable deficiency is that the Privacy Office does not appear to have a process in place to advise components on whether a particular program should be undertaken or technology purchased.[269] Instead, it focuses largely on procedural mechanisms for mitigating privacy issues. As the nongovernmental Electronic Privacy Information Center has observed, the Privacy Office has signed off on all manner of programs and technologies, including fusion centers, whole body imaging, closed-circuit television surveillance, and suspicionless searches of electronic devices at the border. In the course of those approvals, the office has addressed procedural issues, training, and public outreach, but not the basic question of whether these initiatives are compatible with personal privacy.[270]

To be sure, this is not all within the Privacy Office's control: it may not learn of a program under consideration, thus missing the opportunity to weigh in at an early stage, or it may lack the technical expertise to offer sophisticated advice on the potential privacy repercussions of developing technologies. But many of the office's shortcomings seem to have stemmed from a circumscribed view of its role, which may reflect insufficient institutional backing — up through the leadership level — to fulfill its mandate.

Office of Inspector General

The Office of Inspector General layers an important oversight function on top of the Privacy Office and CRCL, and it operates far more independently than the other two offices. Nominated by the president and confirmed by the Senate, the inspector general reports both to Congress and to the DHS secretary.[271] The inspector general has broad investigative powers and must promptly notify Congress of any serious problems within DHS. Interference in OIG investigations by department leadership is generally prohibited.[272] OIG does not provide input as poli-

cies and programs are being developed but examines them after they are implemented.

Armed with this authority, OIG conducts four different types of inquiries: investigations, audits, inspections, and evaluations. Investigations examine specific allegations of misconduct, which may be referred to OIG by CRCL or the Privacy Office. The other types of inquiries address system-level questions and issues. For example, Congress assigned OIG to conduct annual audits of electronic device searches at the border from calendar years 2017 to 2019; two of the three audits have been completed, the last in September 2021.[273] As described in section II, these reviews have overall been critical of the process.

While the results of most inquiries are publicly released, OIG does not release reports of investigations. Instead, the office releases brief summaries of investigations it considers significant.[274] These summaries show that the vast majority of the complaints fielded by OIG from 2002 through 2022 relate to detentions at the southern border.

In a series of inquiries on immigration detention — encompassing audits, evaluations, and inspections — OIG has produced more than 30 reports examining civil rights and civil liberties issues (though these have also been criticized as insufficient).[275] In contrast, its inquiries focused on the programs covered in this report have tended to avoid engaging with these issues. In multiple reports on DHS's watch list programs, for instance, OIG covered the programs' effectiveness but stayed away from obvious profiling and due process concerns. OIG's report on the Quiet Skies program examined TSA's failure to properly administer the program, demonstrate its effectiveness, and adhere to applicable privacy rules, but it did not meaningfully address widespread concerns about bias, including whether the program's targeting criteria relied on race, religion, or national origin.[276] It may be that the inspector general considers these matters to be primarily within the purview of the specialized oversight offices, but those offices' relative lack of influence has meant that these matters have often been given short shrift.[277]

Despite these limitations, OIG's reports provide critical insight and transparency into the programs that are the focus of this report. They are by far the best publicly available source for understanding the functioning of several key DHS programs. And, as described above, OIG has also consistently highlighted DHS's repeated failure to develop metrics to measure the reach and effectiveness of many of its programs.

IV. Recommendations

Based on our review of DHS's record, we have developed a series of recommendations to overhaul the department's approach to counterterrorism, making transparency and the protection of civil rights and civil liberties integral to its efforts while boosting programs' effectiveness. Below we outline five main avenues for reform, which later reports will explore in more detail. In addressing these matters, the department should also seek advice from the Privacy and Civil Liberties Oversight Board, the bipartisan body created by Congress to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.

Strengthen Safeguards Against Profiling

DHS and its state and local partners have often used bias and presumption in lieu of facts to decide whom to surveil, question, and even deport. Some examples are recent, such as the Trump administration's targeting of racial justice protesters, immigrant rights activists, and journalists. Others, such as the questioning of Muslim travelers about their religious beliefs and practices, emerged soon after the department was established. In addition, there is insufficient information about whether — and to what extent — factors such as religion, ethnicity, and national origin play a role in the secretive travel-related risk assessments that DHS undertakes daily.

The DHS secretary should take concrete steps to correct these practices, including by

- expanding DHS policies on nondiscrimination to explicitly cover religion and national origin and eliminating the use of protected characteristics (e.g., race, religion, and ethnicity) except for individual cases in which there is trustworthy information, specific in time and location, that links a person possessing a listed characteristic to a concrete and particular security threat, or as required to administer or enforce U.S. law or executive order (such as those relating to refugees and petitions for asylum); and

- requiring I&A to verify that fusion centers and other entities to which the department provides funding have rules to protect against bias and abide by those rules.

Protect Privacy and Free Expression

Given the huge amount of information about Americans that DHS has already amassed, the department must do more to protect Americans' privacy. Robust privacy and free expression protections would complement strengthened rules against profiling, serving as an additional barrier against abuse.

The secretary should start by reconfiguring DHS's intelligence activities with a dual focus on improving the quality of information and protecting against targeting on the basis of constitutionally protected activity. This effort should include

- reinstituting CRCL review of I&A's intelligence products, which was ended during the Trump administration; and

- instituting a rule that I&A is permitted to create, maintain, or share records of Americans' personal information only if there is reasonable suspicion of criminal activity or planning and the information is relevant and material to that activity or planning. When the information contained in a record concerns First Amendment–protected activities, it must also directly relate to the suspected criminal activity.

As recommended by the DHS general counsel, the secretary should conduct a top-to-bottom review of I&A, which should assess the office's utility and its role in preventing violence. The general counsel's office should also devise a plan to address long-standing challenges, such as inadequate training, the lack of formal and uniform rules on critical issues such as the treatment of U.S. person information in intelligence reports, and the failure to follow best practices in structuring intelligence collection.

In addition, the secretary should direct the Privacy Office and CRCL to

- conduct a wholesale review of the surveillance technologies in use by the department, which should assess the compatibility of these tools with privacy, civil rights, and civil liberties and be made publicly available to the maximum extent possible;

- take the necessary steps to ensure adequate public disclosure of all surveillance technologies used by DHS, including the policies governing the use of these tools, and develop and release an audit plan; and

- develop a formal policy for the department that contains robust protections for individuals' and groups' exercise of First Amendment rights.

The secretary should instruct the department's components to provide the Privacy Office and CRCL with the information they need to carry out these mandates.[278]

Evaluate Efficacy

Time and again, DHS has rolled out programs without evaluating whether they will work and without implementing metrics to measure whether they achieve their stated goals, much less giving serious consideration to their effects on civil rights and civil liberties. Examples include fusion centers, which have hardly contributed to federal counterterrorism efforts; SPOT, the $1.5 billion behavior detection program contradicted by scientific research; Quiet Skies and Silent Partner, the programs tracking both American and foreign travelers on their journeys to, from, and within the United States; the use of social media to assess individuals' threat levels and fitness to enter or remain in the United States; and countering violent extremism programs (now under the CP3 umbrella), which have never been shown to prevent violence.

The secretary should order reviews of these programs and develop a plan for strengthening the processes by which DHS designs and approves initiatives — especially those that are likely to infringe on privacy, civil rights, and civil liberties — to ensure that they are scientifically validated and include appropriate metrics for measuring success before they are implemented or piloted. To support these efforts, the secretary should ensure that the Homeland Security Advisory Council — an appointed body that provides policy analysis, advice, and recommendations — and its subcommittees include nongovernmental experts on privacy, civil rights, and civil liberties.[279]

Ensure Meaningful Transparency

The lack of comprehensive information about the extent of DHS's data holdings hampers the department's formulation of privacy and free speech protections. The secretary should direct a full review of DHS's intake, use, and retention of Americans' data. This process, which could be undertaken by the department's undersecretary for management or its chief data officer, should produce a publicly available taxonomy of what information is collected, where it goes, and to whom it is available.

In addition, while both the Privacy Office and the Office for Civil Rights and Civil Liberties issue multiple public reports, those reports do not always provide useful transparency. The Privacy Office should ensure that its reports allow readers to understand how the department uses data and how information flows between overlapping systems and databases. It may need to develop new products to augment those that are statutorily mandated. Similarly, CRCL's reports to Congress should provide more granular insight into the unit's work. The department's leadership should support rather than inhibit public reporting on serious issues.

Finally, DHS should commit to making the legal bases for its programs clearly delineated and publicly available.

Foster Robust Oversight

The Privacy Office and CRCL should embrace a more robust interpretation of their statutory authorities, and DHS leadership should provide its explicit and public support.

The secretary should empower the Privacy Office to weigh in on *whether* the department should undertake certain initiatives or adopt certain technologies, not just articulate *how* to implement them.[280] CRCL needs more specific leverage points to ensure that its views are seriously considered early in the design and deployment of programs. For example, CRCL has not been able to make effective use of impact assessments. The secretary should make these impact assessments a formal part of the process for approving programs, instruct components to comply with CRCL requests for the information needed to conduct them, and commit to making them public on a regular basis.

The internal influence of both the Privacy Office and CRCL would be further reinforced if the secretary established consequences for a component's failure to notify them of upcoming or ongoing initiatives that implicate privacy, civil rights, or civil liberties, as well as for failure to obtain the offices' affirmative approval for programs.[281]

Finally, the DHS inspector general has provided important insights into several of the programs discussed in this report. OIG should supplement these insights with examinations of the actual impact on privacy, civil rights, and civil liberties of the department's counterterrorism initiatives.

Conclusion

In pursuing its central mission of protecting the United States, DHS has undertaken many misguided programs that have needlessly targeted minority communities and social movements, and it has built the largest governmental store of Americans' personal information with little transparency, oversight, or accountability. While the breadth of management and mandate challenges DHS faces may ultimately require Congress to restructure the department, DHS leadership can take steps now to improve its performance and remedy the accumulated mistakes of the last two decades.

Endnotes

1 A substantial amount of discussion in this report involves harms to Americans. The authors recognize the significant and detrimental consequences of DHS activities for immigrant communities and travelers of other nationalities. This report is not meant to diminish those harms but rather to fill what we perceive to be a gap in policy discussions regarding DHS.

2 In the last two decades, the U.S. government has often treated the actions of individuals in the United States said to be influenced by groups like al-Qaeda and ISIS as international terrorism, even absent any indication of operational links or other concrete connections, on the theory that they promoted a common "foreign" ideology.

3 *Examining the Role of the Department of Homeland Security's Office of Intelligence and Analysis, Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 117th Cong. (2021) (hereinafter *Examining the Role of I&A*) (statement of Mike Sena, president, National Fusion Center Association), https://www.hsgac.senate.gov/imo/media/doc/Testimony-Sena-2021-05-18.pdf. The Implementing Recommendations of the 9/11 Commission Act of 2007 formalized a framework for support of a national network of fusion centers, including through personnel, management support, and technical assistance. 6 U.S.C. § 124(h) (2018).

4 Bureau of Justice Assistance, Department of Justice (hereinafter DOJ) Office of Justice Programs, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, August 2006, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines_law_enforcement.pdf.

5 See Sena, *Examining the Role of I&A*, 2.

6 DHS, *2018 National Network of Fusion Centers Final Report*, 2018 (hereinafter *2018 Final Report*), 2, https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf.

7 Permanent Subcomm. on Investigations, S. Comm. on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers*, October 3, 2021 (hereinafter *Federal Support for Fusion Centers*), 27, https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

8 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 38.

9 North Central Texas Fusion System, "Prevention Awareness Bulletin," February 19, 2009, 4, https://www.privacylives.com/wp-content/uploads/2009/03/texasfusion_021909.pdf.

10 Open the Government, *The Cost of Fear: Long-Cited Abuses Persist at U.S. Government-Funded Post-9/11 Fusion Centers*, accessed December 15, 2021, https://www.openthegovernment.org/dhs-fusion-centers-full-report.

11 Nasser Eledroos and Kade Crockford, "Social Media Monitoring in Boston: Free Speech in the Crosshairs," Privacy SOS (ACLU of Massachusetts), 2018, https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs.

12 See, e.g., Mara Hvistendahl, "Austin Fusion Center Spied on Nonpolitical Cultural Events," *Intercept*, November 30, 2020, https://theintercept.com/2020/11/30/austin-fusion-center-surveillance-black-lives-matter-cultural-events; Micah Lee, "How Northern California's Police Intelligence Center Tracked Protests," *Intercept*, August 17, 2020, https://theintercept.com/2020/08/17/blueleaks-california-ncric-black-lives-matter-protesters; Amanda Peacher, "Why Is the State of Oregon Conducting Intelligence Work?," OPB (Oregon Public Broadcasting), April 26, 2016, https://www.opb.org/news/article/oregon-department-of-justice-intelligence; and Isiah Holmes, "How Should Fusion Centers Be Used During Protests?," *Wisconsin Examiner*, December 22, 2021, https://wisconsinexaminer.com/2021/12/22/how-should-fusion-centers-be-used-during-protests.

13 Policing Project at New York University School of Law, "Press Release: Oregon Sued Over Domestic Spying Operation," December 14, 2021, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/61b89768c753e45b6d99f872/1639487337182/Oregon+TITAN+Lawsuit+Press+Release_12.12.21+FINAL.pdf; Alleen Brown, "Tilting at Windmills: The FBI Chased Imagined Eco-Activist Enemies, Documents Reveal," *Intercept*, August 24, 2020, https://theintercept.com/2020/08/24/fbi-fusion-center-environmental-wind; and Ken Klippenstein, "How Homeland Security Blurs Jurisdictions," *Nation*, December 17, 2020, https://www.thenation.com/article/society/fusion-centers-dhs. Like the FBI and police, fusion centers followed President's Trump lead in exaggerating the threat from leaderless anti-fascists while downplaying the activities of organized violent white supremacists. Ryan Devereaux, "Leaked Documents Show Police Knew Far-Right Extremists Were the Real Threat at Protests, Not 'Antifa,'" *Intercept*, July 15, 2020, https://theintercept.com/2020/07/15/george-floyd-protests-police-far-right-antifa.

14 Ken Klippenstein, "The Madcap Mysteries of Homeland Security," *Nation*, January 26, 2021, https://www.thenation.com/article/society/dhs-fusion-centers.

15 See Jennifer Wadsworth, "BlueLeaks Hack Suggests Bad Intel Fueled SJPD's Violent Response to Recent Protests," *San Jose Inside*, September 16, 2020, https://www.sanjoseinside.com/news/blueleaks-hack-suggests-bad-intel-fueled-sjpds-violent-response-to-recent-protests; and Mara Hvistendahl and Alleen Brown, "Law Enforcement Scoured Protester Communications and Exaggerated Threats to Minneapolis Cops, Leaked Documents Show," *Intercept*, June 26, 2020, https://theintercept.com/2020/06/26/blueleaks-minneapolis-police-protest-fears.

16 Devereaux, "Leaked Documents."

17 For federal government guidelines on compliance verification and auditing, see, e.g., Department of Homeland Security (hereinafter DHS) and DOJ Fusion Process Technical Assistance Program and Services, *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*, June 2010, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/privacy%20civil%20rights%20and%20civil%20liberties%20compliance%20verification%20for%20the%20intelligence%20enterprise.pdf; DOJ Global Advisory Committee, *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, September 2015, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/pcrcl_audit_guidance_for_the_sltt_intelligence_component.pdf; DHS and DOJ Fusion Process Technical Assistance Program and Services, *Fusion Center Privacy Policy Development*, April 2010, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_privacy_policy_development_508compliant.pdf; DOJ Global Justice Information Sharing Initiative, *Privacy, Civil Rights and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*, April 2012, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/privacy_policy_cover_and_body_compliant.pdf; and DOJ Global Justice Information Sharing Initiative and DHS, *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*, December 2011, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/Recommendations%20for%20First%20Amendment-Protected%20Events%20for%20state%20and%20local%20Law%20Enforcement.pdf. Homeland Security Grant Program conditions include maintaining and making public an approved privacy, civil rights, and civil liberties policy; conducting compliance reviews and audits of the policy; ensuring that there is a process for addressing and adjudicating complaints alleging violations of the policy; training all staff on the policy annually; and ensuring that all analytic products are reviewed for privacy and civil rights and civil liberties issues per the policy prior to dissemination and posting to HSIN-Intel, the Homeland Security

Information Network intelligence community. DHS, "Homeland Security Grant Program (HSGP)," accessed December 23, 2021, https://www.dhs.gov/homeland-security-grant-program-hsgp. Fusion centers' publicly available privacy, civil rights, and civil liberties policies are compiled on the National Fusion Center Association website. The list contains 82 policies, generally corresponding in volume to the number of active fusion centers, but it remains unclear whether this compilation reflects all current and operative policies. National Fusion Center Association, "Privacy Policies," accessed December 16, 2021, https://nfcausa.org/privacy-policies.

18 Mike Tipping, "Data Breach Exposes Activities of Maine's Secretive Police Intelligence Agency," *Beacon* (Maine People's Alliance), June 26, 2020, https://mainebeacon.com/data-breach-exposes-activities-of-maines-secretive-police-intelligence-agency. BlueLeaks was the name given to a trove of data stolen from law enforcement websites, including fusion centers, by an anonymous hacker collective in June 2020. See Thomas Brewster, "BlueLeaks: Huge Leak of Police Department Data Follows George Floyd Protests," *Forbes*, June 22, 2020, https://www.forbes.com/sites/thomasbrewster/2020/06/22/blueleaks-huge-leak-of-police-department-data-follows-george-floyd-protests.

19 Tipping, "Data Breach Exposes Activities."

20 Loder v. Maine Intelligence Analysis Center, 2:20-cv-00157-JDL (2020); and Judy Harrison, "Maine State Police Illegally Collecting Data on Residents, Lawsuit Claims," *Bangor Daily News*, May 14, 2020, https://bangordailynews.com/2020/05/14/news/state/state-agency-illegally-collecting-data-on-mainers-claims-trooper-in-whistleblower-suit.

21 Nathan Bernard, "Satirical 'Protest Jobs' Website Was Source of Official Warnings About Leftist Violence," *Mainer News*, July 23, 2020, https://mainernews.com/satirical-protest-jobs-website-was-source-of-official-warnings-about-leftist-violence; Nathan Bernard, "Law Enforcement Distracted by Facetious BLM Tweets as Right-Wing Extremists Run Rampant," *Mainer News*, October 7, 2020, https://mainernews.com/law-enforcement-distracted-by-facetious-blm-tweets-as-right-wing-extremists-run-rampant; and Wadsworth, "BlueLeaks Hack."

22 Alice Speri, "The Defund Police Movement Takes Aim at Fusion Centers and Mass Surveillance," *Intercept*, April 21, 2021, https://theintercept.com/2021/04/21/maine-defund-police-fusion-centers-mass-surveillance.

23 An Act to End the Maine Information and Analysis Center Program, L.D. 1278, 130th Sess. (2021); and "Bill to Close State Police 'Fusion Center' Fails in Senate," *U.S. News & World Report*, June 15, 2021, https://www.usnews.com/news/best-states/maine/articles/2021-06-15/bill-to-close-state-police-fusion-center-fails-in-senate.

24 Michael Price, *National Security and Local Police*, Brennan Center for Justice, December 10, 2013, 18, https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf; and DHS, *2018 Final Report*. For federal government guidelines on compliance verification and auditing, see DHS and DOJ Fusion Process Technical Assistance Program and Services, *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*; and Global Advisory Committee, *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*.

25 "Interlocal Cooperation Agreement for the Austin Regional Intelligence Center (ARIC)," accessed December 15, 2021, https://www.austintexas.gov/edims/document.cfm?id=137700.

26 Daniela Hargus et al., *The Silicon Hills Have Eyes: How ARIC Fusion Center Surveillance Makes Austin Less Safe*, Grassroots Leadership, July 2021, 7, https://grassrootsleadership.org/sites/default/files/reports/silicon_hills_have_eyes_report_-_final_1.pdf.

27 Hargus et al., *Silicon Hills Have Eyes*, 11.

28 *Loder v. Maine Intelligence Analysis Center*; Harrison, "Maine State Police"; Bernard, "Satirical 'Protest Jobs' Website"; Bernard, "Law Enforcement Distracted"; and Wadsworth, "BlueLeaks Hack Suggests Bad Intel."

29 DHS and DOJ Fusion Process Technical Assistance Program and Services to Oregon Terrorism Information Threat Assessment Network, memorandum, January 22, 2014, 2, https://aclu-or.org/sites/default/files/Oregon-Memo_FC-Audit-2014_web.pdf.

30 Complaint for Declaratory Judgment and Injunctive Relief, Ka'Ila Farrell-Smith et al. v. Oregon Department of Justice et al., no. 21CV47809, December 14, 2021, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/61bb7484b5d3234af35ca694/1639675023280/2021-12-14+Oregon+Complaint+FILE-STAMPED.pdf.

31 Open the Government, *Cost of Fear*.

32 Suzanne M. Bump, *Official Audit Report: Department of State Police — Fusion Center Operations*, Office of the State Auditor, Commonwealth of Massachusetts, January 18, 2019, 6–7, https://www.mass.gov doc/a-pdf-copy-of-the-audit-of-the-department-of-state-police-fusion-center-operations/download.

33 Government Accountability Office (hereinafter GAO), "Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective," March 13, 2013, 7, https://www.gao.gov/products/gao-13-233. See generally DHS, "Nationwide SAR Initiative (NSI)," accessed December 23, 2021, https://www.dhs.gov/nationwide-sar-initiative-nsi/nsi-partners; and Office of the Director of National Intelligence (hereinafter ODNI), "A Brief History of the Information Sharing Environment (ISE)," October 2015, https://www.hsdl.org/?abstract&did=812949.

34 Price, *National Security and Local Police*, 27–28; ODNI, "Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)," version 1.5.5, February 2015 (hereinafter "ISE Functional Standard SAR"), https://www.dhs.gov/sites/default/files/publications/15_0223_NSI_ISE-Functional-Standard-SAR.pdf; and 28 C.F.R. § 23.20(c) (the federal rule requiring the inclusion of personally identifiable information connected to criminal intelligence information be supported by reasonable suspicion).

35 ODNI, "ISE Functional Standard SAR," 15, 41–51.

36 Mary Ellen Callahan, *Privacy Impact Assessment for the Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative*, DHS Privacy Office, November 17, 2010, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-sar-update-20101117_0.pdf. This PIA was updated in 2015. See Karen L. Neuman, *Privacy Impact Assessment for the Department of Homeland Security Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Initiative*, DHS/ALL/PIA-032(a), DHS Privacy Office, May 12, 2015, https://www.dhs.gov/sites/default/files/publications/PIA%2C%20DHS%20-%20DHS%20ISE%20SAR%2C%2020150512%2C%20PRIV%20Final%20%5Bsigned%5D_0.pdf.

37 Mike German and Jay Stanley, "Fusion Center Update," ACLU, July 2008, https://www.aclu.org/files/pdfs/privacy/fusion_update_20080729.pdf.

38 *Sixteen Years After 9/11: Assessing Suspicious Activity Reporting Efforts*, *Before the H. Comm. on Homeland Security*, 115th Cong. (2017) (written testimony of Robin Taylor, I&A acting deputy undersecretary for intelligence operations), https://www.dhs.gov/news/2017/09/13/written-testimony-ia-house-homeland-security-subcommittee-counterterrorism-and-0.

39 Taylor, *Sixteen Years After 9/11*. Even these numbers should be taken with a grain of salt. Given the low standard used by the FBI for opening investigations — with the lowest level not requiring any criminal suspicion — linkage to an FBI investigation means very little. See Michael German, "Standards for Opening an FBI Investigation So Low They Make the Statistic Meaningless," Brennan Center for Justice, May 2, 2017, https://www.brennancenter.org/our-work/analysis-opinion/standards-opening-fbi-investigation-so-low-they-make-statistic.

Similarly, the fact that an SAR's subject is on a watch list scarcely suggests that their inclusion pertains to terrorism, considering long-standing issues relating to those lists' overbreadth and reliability (as discussed further in section II).

40 The Los Angeles fusion center, for example, kept 98 percent of its suspicious activity reports between 2008 and 2010, despite the fact that only 2 percent were determined to have a connection to terrorism. Price, *National Security and Local Police*, 14.

41 As discussed in section III, the assessment conducted by CRCL fell far short of this goal. Other evaluations have addressed the functioning of fusion centers. See, e.g., GAO, "Information Sharing: Additional Actions Could Help"; DHS Office of Inspector General (hereinafter OIG), *Relationships Between Fusion Centers and Emergency Operations Centers*, December 6, 2011, 1, https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_12-15_Dec11.pdf; and GAO, *Information Sharing: DHS Is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Centers*, November 4, 2014, https://www.gao.gov/assets/gao-15-155.pdf.

42 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 1, 31. Even a 2013 report from the House Committee on Homeland Security issued as a rebuttal to the Senate report found that DHS's performance measures failed "to provide a complete picture . . . of how fusion center–gathered information affects Federal terrorism or criminal cases or other homeland security mission areas," a problem that has not been addressed. Michael T. McCaul and Peter T. King, *Majority Staff Report on the National Network of Fusion Centers*, H. Comm. on Homeland Security, July 2013, 7, https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/staff-report-on-fusion-networks-2013.pdf.

43 Cyrus Farivar, "20 Years After 9/11, 'Fusion Centers' Have Done Little to Combat Terrorism," NBC News, September 10, 2021, https://www.nbcnews.com/business/business-news/20-years-after-9-11-fusion-centers-have-done-little-n1278949; and Speri, "Defund Police Movement."

44 DHS, *2018 Final Report*, 4. In 2020, the DHS Field Engagement Accountability Act became law. Passed roughly two decades after fusion centers were first stood up, the legislation requires DHS to come up with and update every five years a strategy for information sharing with fusion centers, and better measure the performance of its field personnel deployed at them, albeit without specifying specific metrics for doing so. But it does not require DHS to evaluate how well fusion centers are actually working to prevent terrorism and is silent on addressing civil rights and liberties issues they have posed. Pub. L. No. 116-116, 134 Stat. 111 (2020).

45 6 U.S.C. § 121 (2018).

46 Office of Intelligence and Analysis (hereinafter I&A), *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines*, DHS, January 19, 2017, 3–4, https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf. I&A's intelligence oversight guidelines divide its "authorized intelligence missions" into two categories: "national missions" related to "foreign security threats" and "departmental missions" related to "threats to homeland security." While the categories appear intended to distinguish between threats from outside the United States and threats from within it, they may not correspond with operational realities (e.g., a U.S.-born and resident person being investigated for "international terrorism" due to an alleged connection to or influence from a designated foreign terrorist organization). The guidelines recognize that "I&A activities can be in furtherance of both national and departmental missions simultaneously." Intelligence activities are authorized when I&A officials have a "reasonable belief" that they support one or more of these national or departmental missions.

47 I&A, *Intelligence Oversight Program and Guidelines*, 2 (emphasis added). In May 2019, then–acting Secretary of Homeland Security Kevin McAleenan issued a memo to all DHS employees reiterating limits on the targeting of First Amendment–protected activities, but the practical impact of such guidance is dubious given numerous subsequent reported instances of abuse. DHS, "Information Regarding First Amendment Protected Activities," memorandum from Kevin K. McAleenan, acting secretary of homeland security, to all DHS employees, May 17, 2019, https://www.dhs.gov/sites/default/files/publications/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019.pdf.

48 According to the *New York Times*, DHS also deployed aircraft to surveil the summer 2020 protests against police violence in more than 15 cities across the country. Zolan Kanno-Youngs, "U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance," *New York Times*, June 19, 2020, https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html. The footage was broadcast live to a CBP control room and fed into a DHS-managed digital network that is accessible to federal agencies and local police departments in criminal investigations. Kanno-Youngs, "U.S. Watched George Floyd Protests" (likely referencing DHS, *Privacy Impact Assessment for the Aircraft Systems*, DHS/CBP/PIA-018, September 9, 2013, 9, 17, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-aircraft-systems-20130926.pdf).

49 Steve Vladeck and Benjamin Wittes, "DHS Authorizes Domestic Surveillance to Protect Statues and Monuments," *Lawfare* (blog), July 20, 2020, https://www.lawfareblog.com/dhs-authorizes-domestic-surveillance-protect-statues-and-monuments; and Exec. Order No. 13,933, "Protecting American Monuments, Memorials, and Statues and Combating Recent Criminal Violence," 85 Fed. Reg. 40081 (June 26, 2020), https://www.federalregister.gov/documents/2020/07/02/2020-14509/protecting-american-monuments-memorials-and-statues-and-combating-recent-criminal-violence. For more on racial justice demonstrations during the summer of 2020, see Michael D. Shear, "Trump Issues Executive Order Targeting Vandalism Against Monuments," *New York Times*, June 26, 2020, https://www.nytimes.com/2020/06/26/us/politics/trump-monuments-executive-order.html.

50 Rep. Adam B. Schiff, chair of the H. Permanent Select Comm. on Intelligence, to Chad F. Wolf, acting secretary of homeland security, and Brian Murphy, acting undersecretary, I&A, July 22, 2020, https://intelligence.house.gov/uploadedfiles/20200722hpsci_chm_letter_to_dhs.pdf.

51 The department acknowledged the inappropriateness of these actions when they came to light and said that it would "discontinue" collecting information on members of the press. Shane Harris, "DHS Compiled 'Intelligence Reports' on Journalists Who Published Leaked Documents," *Washington Post*, July 30, 2020, https://www.washingtonpost.com/national-security/dhs-compiled-intelligence-reports-on-journalists-who-published-leaked-documents/2020/07/30/5be5ec9e-d25b-11ea-9038-af089b63ac21_story.html. At the time of this report's publication, the DHS inspector general's report had not been publicly released.

52 DHS Office of the General Counsel, *Report on DHS Administrative Review into I&A Open Source Collection and Dissemination Activities During Civil Unrest, Portland, Oregon, June Through July 2020*, DHS, January 6, 2021 (hereinafter *Report on DHS Administrative Review into I&A*), 8, http://cdn.cnn.com/cnn/2021/images/10/01/internal.review.report.20210930.pdf.

53 Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 64. The instruction was made even though I&A did not have any evidence supporting such a characterization. The term was later modified to "threat actors who are *probably* motivated by Anarchist or ANTIFA" and made optional after pushback from I&A's associate general counsel and another senior official, though analysts' concerns about the credibility of connected intelligence products persisted. Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 66 (emphasis in original).

54 OIG, "Whistleblower Reprisal Complaint," DHS, September 8, 2020, 14, https://int.nyt.com/data/documenttools/homeland-security-whistleblower/0819ec9ee29306a5/full.pdf.

55 Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 70.

56 Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 68–69. Among other issues, the review found that I&A analysts could not distinguish a "true threat" from chatter online; that personnel misused the word "incite"; and that even the head of the Current and Emerging Threats Center (the I&A component leading the effort in Portland, Oregon, which aims to "provide[] 24/7 indication and warning of threats directed against the Homeland") did not know that "counterintelligence," an elementary intelligence term, involved a foreign component. Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 21, 27; and DHS, "Other Intelligence Elements," accessed January 24, 2022, https://www.dhs.gov/other-intelligence-elements. I&A has since implemented a mandatory two-week training program for intelligence collectors. Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 68. How effective the training will be remains to be seen. Training issues and I&A's failure to properly measure the effectiveness of efforts to improve personnel skills are long-standing concerns. GAO, *DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges*, June 4, 2014, 31–32, https://irp.fas.org/agency/dhs/dhs-intel.pdf.

57 Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 22, 33, 73. The line between proactive threat detection and strategic intelligence measures can be blurry, however. For example, in 2021, I&A rolled out an initiative to identify online "narratives" believed to incite violence — an effort that will inevitably flag individuals as threats as well. *Racially and Ethnically Motivated Violent Extremism: The Transnational Threat, Hearing Before the H. Comm. on Homeland Security Subcomm. on Intelligence and Counterterrorism*, 117th Cong. (2021) (oral testimony of John Cohen, assistant DHS secretary for counterterrorism and threat prevention); DHS, "Summary of Terrorism Threat to the U.S. Homeland," National Terrorism Advisory System Bulletin, August 13, 2021, https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-august-13-2021; and Ken Dilanian and Julia Ainsley, "DHS Weighing Major Changes to Fight Domestic Violent Extremism, Say Officials," NBC News, March 25, 2021, https://www.nbcnews.com/politics/national-security/dhs-weighing-huge-changes-fight-domestic-violent-extremism-say-officials-n1262047.

58 Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 30. While I&A's guidelines do not require these markings for publicly available information, the unit had historically taken what the review called "a more prudent course of action" and "minimized" the naming of Americans. After the Portland incident, part of I&A issued a policy to its workforce requiring masking of personally identifiable information except where unmasking is permitted by other authorities; however, the policy does not apply to all parts of I&A. Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 30, 70–71. And these markings are not permanent; when an entity wants to learn the identity of an individual that has been redacted in an intelligence report, it can submit a request articulating a need for the information. DHS, "Requests for Identities of U.S. Persons in Disseminated Intelligence Reports," no. 264-01-010, February 24, 2020, https://www.intel.gov/assets/documents/702%20Documents/oversight/DHS_ICPG_107_1_Unmasking_Procedures_022420OCR.pdf.

59 Office of the General Counsel, *Report on DHS Administrative Review into I&A*, 71.

60 OIG, *I&A Identified Threats Prior to January 6, 2021, but Did Not Issue Any Intelligence Products Before the U.S. Capitol Breach*, March 2022, https://www.oig.dhs.gov/sites/default/files/assets/2022-03/OIG-22-29-Mar22-Redacted.pdf.

61 OIG, *I&A Identified Threats Prior to January 6, 2021*, 9, 20.

62 OIG, *I&A Identified Threats Prior to January 6, 2021*, 11, 14, 19.

63 OIG, *I&A Identified Threats Prior to January 6, 2021*, 21.

64 OIG, *I&A Identified Threats Prior to January 6, 2021*, 8.

65 *Violent Extremism and Terrorism: Examining the Threat to Houses of Worship and Public Spaces, Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 117th Cong. (2022) (testimony of Stephanie Dobitsch, deputy undersecretary for intelligence enterprise operations, DHS), https://www.hsgac.senate.gov/hearings/violent-extremism-and-terrorism-examining-the-threat-to-houses-of-worship-and-public-spaces.

66 "Probe of Nation of Islam Improper," *Columbus Dispatch*, updated December 17, 2009, https://www.dispatch.com/story/news/2009/12/17/probe-nation-islam-improper/23566463007.

67 I&A, *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment*, April 7, 2009 (hereinafter *Rightwing Extremism*), https://fas.org/irp/eprint/rightwing.pdf; Teddy Davis and Ferdous Al-Faruque, "Napolitano Facing Republican Calls for Her Ouster," ABC News, April 23, 2009, https://abcnews.go.com/Politics/story?id=7412992; and Rep. Bennie Thompson, chair, H. Comm. on Homeland Security, to Janet Napolitano, secretary of homeland security, April 14, 2009, https://www.facingsouth.org/sites/default/files/Thompson_Letter.pdf.

68 Spencer Ackerman, "DHS Crushed This Analyst for Warning About Far-Right Terror," *Wired*, August 7, 2012, https://www.wired.com/2012/08/dhs.

69 I&A, *Rightwing Extremism*, 2.

70 Jason Leopold, "How the Government Monitored Twitter During Baltimore's Freddie Gray Protests," *VICE*, May 18, 2016, https://www.vice.com/en/article/5gqmbq/riot-police-v23n3. I&A's surveillance of the protests yielded little useful information — it disseminated a tweet from an obscure Twitter account apparently urging violence on behalf of ISIS, and another that included a photo with redacted Arabic text, for example. The office also apparently produced a report referred to as the "Race Paper," which has never been publicly disclosed. Center for Constitutional Rights, "Briefing Guide: Color of Change v. FBI and DHS," May 16, 2018, https://ccrjustice.org/briefing-guide-color-change-v-fbi-dhs.

71 Curtis Waltman, "Even Amid Emerging White Supremacist Threat, Homeland Security Is Still Caught Up on Leftist Groups," Muckrock, August 22, 2017, https://www.muckrock.com/news/archives/2017/aug/22/dhs-mayday.

72 Ryan Devereaux, "Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests," *Intercept*, April 29, 2019, https://theintercept.com/2019/04/29/family-separation-protests-surveillance.

73 DHS, "Center for Prevention Programs and Partnerships," accessed December 16, 2021, https://www.dhs.gov/CP3.

74 For more information on these programs, see Harsha Panduranga, *Community Investment, Not Criminalization*, Brennan Center, June 17, 2021, 24, 29, https://www.brennancenter.org/sites/default/files/2021-06/2021_06_DHS_Targeted_Prevention.pdf; and Faiza Patel and Megan Koushik, *Countering Violent Extremism*, Brennan Center for Justice, March 26, 2017, 34, https://www.brennancenter.org/sites/default/files/publications/Brennan%20Center%20CVE%20Report_0.pdf.

75 DHS, *Fiscal Year 2016 Countering Violent Extremism Grant Program: Preliminary Report on Programmatic Performance*, March 26, 2020, 31, https://www.dhs.gov/sites/default/files/publications/20_0326_tvtp_preliminary-report-programmatic-performance-fy16-cve-grants_1.pdf.

76 In 2020, for example, DHS awarded $10 million to 29 organizations, 13 of which funded law enforcement or public safety entities directly. Another seven grant recipients had some relationship to law enforcement (e.g., they listed the FBI as a partner). In 2021, DHS awarded $20 million to 37 organizations. DHS, "Targeted Violence and Terrorism Prevention Grant Program," last updated September 28, 2021 (hereinafter "TVTP Grant Program 2021"), https://www.dhs.gov/tvtpgrants; and Panduranga, *Community Investment, Not Criminalization*, appendix. While fewer grants (10) were awarded directly to law enforcement or public safety entities, 28 grants provide at least some funds for bolstering pre-criminal identification

and referral frameworks incorporating law enforcement. Some grants went to departments with a history of civil rights and liberties transgressions, including the Los Angeles Police Department. See, e.g., Mary Pat Dwyer and José Guillermo Gutiérrez, "Documents Reveal LAPD Collected Millions of Tweets from Users Nationwide," Brennan Center for Justice, December 15, 2021, https://www.brennancenter.org/our-work/analysis-opinion/documents-reveal-lapd-collected-millions-tweets-users-nationwide.

77 White House, "Empowering Local Partners to Prevent Violent Extremism in the United States," August 2011, https://obamawhitehouse.archives.gov/sites/default/files/empowering_local_partners.pdf. In 2014, the DOJ announced CVE pilot programs in Boston, Los Angeles, Minneapolis, and Montgomery County, Maryland. DOJ, "Press Release: Attorney General Holder Announces Pilot Program to Counter Violent Extremists," September 15, 2014, https://www.justice.gov/opa/pr/attorney-general-holder-announces-pilot-program-counter-violent-extremists.

78 Rupa Shenoy, "Critics Say Biden's Plan to Combat Domestic Extremism Repeats Past Mistakes," *World*, July 1, 2021, https://theworld.org/stories/2021-07-01/critics-say-biden-s-plan-combat-domestic-extremism-repeats-past-mistakes.

79 Patel and Koushik, *Countering Violent Extremism*, 9–16.

80 The initiative is connected to a federal grants program that retains the former title. DHS, "TVTP Grant Program 2021."

81 Brian A. Jackson et al., *Practical Terrorism Prevention: Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence*, Homeland Security Operational Analysis Center (RAND Corporation), 2019, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2600/RR2647/RAND_RR2647.pdf (emphasis added); and Panduranga, *Community Investment, Not Criminalization*, 13–17.

82 Panduranga, *Community Investment, Not Criminalization*, 13–15.

83 Panduranga, *Community Investment, Not Criminalization*, 24.

84 Libby Nelson, "The Hidden Racism of School Discipline, in 7 Charts," *Vox*, October 31, 2015, https://www.vox com/2015/10/31/9646504/discipline-race-charts; Derrick Darby and John L. Rury, "When Black Children Are Targeted for Punishment," *New York Times*, September 25, 2017, https://www.nytimes.com/2017/09/25/opinion/black-students-little-rock-punishment.html; and Madeline Will, "Teachers Are as Racially Biased as Everybody Else, Study Shows," *Education Week*, June 9, 2020, https://www.edweek.org/teaching-learning/teachers-are-as-racially-biased-as-everybody-else-study-shows/2020/06.

85 *DHS Office for Targeted Violence and Terrorism Prevention: FY2016 Grant Evaluations October 2021* (hereinafter *FY2016 Grant Evaluations*), https://www.dhs.gov/sites/default/files/2021-12/21_1220_st_CVE_Final_Report-10-4-21_0.pdf. Unfortunately, recent GAO reviews of these grants also failed to delve into whether the programs were meeting their goal of violence prevention. A February 2021 audit, for example, criticized DHS's failure to determine effectiveness, but focused on several grantees' failure to provide required information rather than the more basic question of whether the approach was a credible one. GAO, *Countering Violent Extremism: DHS Needs to Improve Grants Management and Data Collection*, February 2021, https://www.gao.gov/assets/720/712452.pdf. See also GAO, *Countering Violent Extremism: DHS Can Further Enhance Its Strategic Planning and Data Governance Efforts*, July 2021, https://www.gao.gov/assets/gao-21-507.pdf.

86 DHS, *FY2016 Grant Evaluations*, 2.

87 Consolidated Appropriation Act of 2022, H.R. 2471, 117th Cong. (2022). The administration has requested $20 million for the Targeted Violence and Terrorism Prevention grant program in 2023. Alejandro Mayorkas, *Fiscal Year (FY) 2023 Budget in Brief*, DHS, 2022, 97, https://www.dhs.gov/sites/default/files/2022-03/22-%201835%20-%20FY%202023%20Budget%20in%20Brief%20FINAL%20with%20Cover_Remediated.pdf.

88 Chappell Lawson and Alan Bersin, "The Future of Homeland Security," 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), 303.

89 The creation of a biometric entry-exit system was one of the main recommendations of the 9/11 Commission and formed part of a 2002 law on border security and visa reform, the Enhanced Border Security and Visa Entry Reform Act. In 2004, DHS began collecting fingerprints and a digitized photograph from all foreign travelers entering at U.S. international airports. In 2017, the department replaced fingerprint scans with mandatory facial recognition for all incoming foreign nationals, as well as for U.S. passport holders arriving at U.S. international airports on a voluntary basis. Homeland Security Advisory Council, *Final Report of the Biometrics Subcommittee*, DHS, November 12, 2020, 9, https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.

90 While CBP Directive No. 3340-049A requires agents to disconnect devices from the internet during "basic" searches, cached social media data and even messaging data may still be accessible. CBP, "CBP Directive No. 3340-049A: Border Search of Electronic Devices," DHS, January 4, 2018, 10, https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf. Moreover, according to a 2018 report from DHS's inspector general, CBP's field officers had not consistently disabled network connections in devices before searches, even after the issuance of a 2017 memo instructing officers to do so. OIG, *CBP's Searches of Electronic Devices at Ports of Entry — Redacted*, DHS, December 3, 2018, 9, https://www.oig.dhs.gov/sites/default/files/assets/2018-12/OIG-19-10-Nov18.pdf.

91 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.

92 See U.S. Customs and Border Protection (hereinafter CBP), "Frequently Asked Questions: Receipt of Passenger Name Record Data," DHS, September 13, 2019, 2–3, https://www.cbp.gov/sites/default/files/assets/documents/2020-May/PNR-FAQs-%28508-compliant%29.pdf; and Edward Hasbrouck, "What's in a Passenger Name Record (PNR)?," *Practical Nomad* (blog), accessed December 22, 2021, https://hasbrouck.org/articles/PNR.html. The Privacy and Civil Liberties Oversight Board, an independent federal agency, has announced that it is conducting an oversight project on the use of PNR, though no information is available about the status or expected completion date. Privacy and Civil Liberties Oversight Board, "Projects," accessed December 21, 2021, https://www.pclob.gov/Projects.

93 Byron Tau and Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement," *Wall Street Journal*, February 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600. See also Joseph Cox, "How an ICE Contractor Tracks Phones Around the World," *VICE*, December 3, 2020, https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps; Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *VICE*, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; and Joseph Cox, "CBP Refuses to Tell Congress How It Is Tracking Americans Without a Warrant," *VICE*, October 23, 2020, https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant.

94 See Charles Levinson, "Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones," *Protocol*, March 5, 2020, https://www.protocol.com/government-buying-location-data. Little is known about the specifics, as Babel Street's contracts require that Locate X data remain confidential and not be cited in court or investigation-related documents. CBP's and ICE's privacy impact assessments only authorize the use of location data to detect activities or the presence of — but not to identify — individuals in areas of interest. Philip S. Kaplan, *Privacy Impact Assessment Update for the*

Border Surveillance Systems (BSS), DHS/CBP/PIA-022(a), DHS Privacy Office, August 21, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp022-bss-september2018.pdf; and Philip S. Kaplan, *Privacy Impact Assessment for the Data Analysis System (DAS)*, DHS/ICE DAS/PIS-048, DHS Privacy Office, September 29, 2017 (hereinafter *PIA for DAS*), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-das-september2017.pdf.

95 Tau and Hackman, "Federal Agencies Use Cellphone Location Data" (citing a statement in which an ICE spokesperson stated, "We do not discuss specific law-enforcement tactics or techniques, or discuss the existence or absence of specific law-enforcement-sensitive capabilities"). See also Joseph Cox, "Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal," *VICE*, August 25, 2020, https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs; Sen. Ron Wyden et al. to Joseph V. Cuffari, DHS inspector general, October 23, 2020, https://www.wyden.senate.gov/imo/media/doc/102320%20Wyden%20Warren%20Brown%20Markey%20Schatz%20Letter%20RE%20CBP%20Phone%20Tracking.pdf; and Joseph V. Cuffari, DHS inspector general, to Sen. Ron Wyden et al., November 25, 2020, https://www.wyden.senate.gov/imo/media/doc/OIG%20Response%20Wyden%20Warren%20Brown%20Markey%20Schatz%20Letter%20RE%20CBP%20Phone%20Tracking.pdf. As of February 2022, the results of the inspector general's audit — or even whether the audit has been formally initiated — had not been made public. A group of senators and representatives, including the chair of the House Committee on Oversight and Reform, has also sought information and documents from Venntel. H. Comm. on Oversight and Reform to Chris Gildea, president of Venntel, June 24, 2020, https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2020-06-24.CBM%20Warren%20Wyden%20DeSaulnie%20to%20Venntel%20re%20Mobile%20Phone%20Location%20Data.pdf.

96 Carpenter v. United States, 138 S. Ct. 2206 (2018).

97 J. Russell George, treasury inspector general for tax administration, Internal Revenue Service, to Sens. Ron Wyden and Elizabeth Warren, February 18, 2021, https://s.wsj.net/public/resources/documents/Response.pdf.

98 ExpressVPN, "Investigation Xoth: Smartphone Location Tracking," accessed December 23, 2021, https://www.expressvpn.com/digital-security-lab/investigation-xoth; and Kaplan, *PIA for DAS*, 13 (stating that "when information is gathered by these vendors from open (i.e., publicly available) sources, individuals may have no notice or only constructive notice").

99 See, e.g., Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

100 See ExpressVPN, "Investigation Xoth."

101 Jonathan R. Cantor, *Privacy Impact Assessment Update for the Electronic System for Travel Authorization (ESTA)*, DHS/CBP/PIA-007(g), DHS Privacy Office, September 1, 2016, 2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-september2016.pdf; and Office of Management and Budget, "Notice of Office of Management and Budget Action," December 19, 2016, https://www.reginfo.gov/public/do/DownloadNOA?requestID=275860.

102 Brennan Center for Justice, "Doc Society v. Blinken," accessed December 16, 2021, https://www.brennancenter.org/our-work/court-cases/doc-society-v-blinken.

103 See, e.g., Eyder Peralta, "Lost in Translation: Because of Twitter Joke, Brits Denied Entry to U.S.," NPR, January 30, 2012, https://www.npr.org/sections/thetwo-way/2012/01/30/146092724/lost-in-translation-because-of-twitter-joke-brits-denied-entry-to-u-s; and Nathan Bernard, "Maine Spy Agency Spread Far-Right Rumors of BLM Protest Violence," *Mainer News*, July 7, 2020, https://mainernews.com/maine-spy-agency-spread-far-right-rumors-of-blm-protest-violence.

104 Privacy Office, "Privacy Threshold Analysis Version Number: 01-2014," DHS, January 2014, 4n2, https://www.brennancenter.org/sites/default/files/2022-02/PTA%20for%20OI%20and%20OPR.pdf; and Privacy Office, "Privacy Threshold Analysis (PTA) Version Number: 04-26," DHS, March 14, 2017, 8, https://www.brennancenter.org/sites/default/files/2022-03/PTA%202017%20SM%20as%20SPII.pdf (noting that social media handles constitute "stand-alone Sensitive Personally Identifiable Information").

105 U.S. Citizenship and Immigration Services, "Social Media," in *U.S. Citizenship and Immigration Services Briefing Book*, 181, https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf. For further discussion of the pilot programs, see Faiza Patel et al., *Social Media Monitoring*, Brennan Center for Justice, updated March 11, 2020, 30–31, https://www.brennancenter.org/our-work/research-reports/social-media-monitoring.

106 OIG, *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-Term Success (Redacted)*, DHS, February 27, 2017, https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.

107 Office of Information and Regulatory Affairs, "Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms," Office of Management and Budget, April 2, 2021, https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202007-1601-001. In November 2021, DHS issued a notice that it intended to undertake a narrower collection, converting the optional collection of social media identifiers from individuals traveling from countries covered by the visa waiver program into a mandatory collection. It issued a supplementary notice in February 2022, reopening the comment period. At the time of this report's publication, that rule had not yet been finalized. CBP, "Arrival and Departure Record, Nonimmigrant Visa Waiver Arrival/Departure, Electronic System for Travel Authorization (ESTA)," 86 Fed. Reg. 64508, November 18, 2021, https://www.federalregister.gov/documents/2021/11/18/2021-25147/arrival-and-departure-record-nonimmigrant-visa-waiver-arrivaldeparture-electronic-system-for-travel; and CBP, "Arrival and Departure Record, Nonimmigrant Visa Waiver Arrival/Departure, Electronic System for Travel Authorization (ESTA)," 87 Fed. Reg. 36, 10223, https://www.govinfo.gov/content/pkg/FR-2022-02-23/pdf/2022-03814.pdf.

108 These searches take two forms: "basic" searches, in which agents view information that "would ordinarily be visible by scrolling through the phone manually," and more intrusive "advanced" searches, in which an officer connects equipment to the device to download, review, copy, and analyze its contents. Court decisions and changes in departmental policy have tightened the standards for some of these searches, but agents may still conduct basic searches for any reason or for no reason at all. Philip S. Kaplan, *Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices*, DHS/CBP/PIA-008(a), DHS Privacy Office, January 4, 2018, 6, https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf; CBP, "Directive 3340-049A: Border Search of Electronic Devices," 4–5. If there is a "national security concern" or reasonable suspicion of a violation of law, border officers may also perform an advanced search.

109 CBP, "CBP Enforcement Statistics Fiscal Year 2002," DHS, accessed December 16, 2021, 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.

110 Karen Zraick and Mihir Zaveri, "Harvard Student Says He Was Barred from U.S. over His Friends' Social Media Posts," *New York Times*, August 27, 2019, https://www.nytimes.com/2019/08/27/us/harvard-student-ismail-ajjawi.html.

111 OIG, *CBP's Searches of Electronic Devices*, 5–7. In addition, the systems used and data collected during searches were in many cases

not adequately managed and secured. OIG, *CBP's Searches of Electronic Devices*, 7–8.

112 OIG, *CBP's Searches of Electronic Devices*, 9.

113 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. In addition, while the privacy impact assessment for electronic device searches requires periodic audits, there is little information on what these audits entail or the results. In February 2019, the Electronic Privacy Information Center sued for the release of this information, but nothing has been released yet. Electronic Privacy Information Center v. U.S. Customs and Border Protection, No. 1:2019cv00279 (D.D.C., filed February 1, 2019). For more on the case, see Electronic Privacy Information Center (hereinafter EPIC), "EPIC v. CBP (Border Search Audits of Electronic Devices)," accessed December 16, 2021, https://epic.org/foia/dhs/cbp/electronic-device-search-audit.

114 Cyrus Farivar, "Woman: My iPhone Was Seized at Border, Then Imaged — Feds Must Now Delete Data," *Ars Technica*, August 23, 2018, https://arstechnica.com/tech-policy/2018/08/woman-my-iphone-was-seized-at-border-then-imaged-feds-now-must-delete-data; Ryan Devereaux, "Journalists, Lawyers, and Activists Working on the Border Face Coordinated Harassment from U.S. and Mexican Authorities," *Intercept*, February 8, 2019, https://theintercept.com/2019/02/08/us-mexico-border-journalists-harassment; and Carrie DeCell, "Warrantless Border Searches: The Officer 'Searched Through Every Email and Intimate Photos of My Wife,'" *Just Security*, December 22, 2017, https://www.justsecurity.org/50095/laptop-cellphone-searches-border. While the DHS inspector general is currently conducting an audit on electronic device searches, it is not clear whether these allegations will be covered. OIG, "Ongoing Projects," DHS, accessed December 16, 2021, https://www.oig.dhs.gov/reports/ongoing-projects?field_project_dhs_component_value=All&field_project_mission_value=8.

115 Terrorist Screening Center, "Frequently Asked Questions," FBI, January 2017, https://www.fbi.gov/file-repository/terrorist-screening-center-frequently-asked-questions.pdf/view.

116 Elhady v. Kable, No. 1:16-cv-00375-AJT-JFA (E.D. Va. 2019) (memorandum opinion and order), 4, https://int.nyt.com/data/documenthelper/1689-terror-watchlist-ruling/75cd50557652ad0b-fa2a/optimized/full.pdf.

117 A subset of the people on the TSDB are on the No Fly List, which prevents them from boarding planes to or in the United States. The use of the No Fly List to prevent Americans from boarding planes has been challenged in several court cases. See, e.g., Latif v. Holder, 28 F. Supp. 3d 1134, 1149, 1154 (D. Or. 2014); Kashem v. Barr, 941 F. 3d 358, 391 (9th Cir. 2019); Mohamed v. Holder, 995 F. Supp. 2d 520, 528 (E.D. Va. 2014); and Mohamed v. Holder, 266 F. Supp. 3d 868 (E.D. Va. 2017).

118 See Privacy Office, *2019 Data Mining Report to Congress*, DHS, December 2, 2020, 12, 14, https://www.dhs.gov/sites/default/files/publications/2019_data_mining_report_final_12-2-20.pdf.

119 CBP, "Frequently Asked Questions," 2–3. The Advance Passenger Information System also requires airlines to send passenger information to DHS. CBP, "Fact Sheet: APIS," DHS, November 12, 2013, https://www.cbp.gov/sites/default/files/documents/apis_factsheet_3.pdf.

120 With respect to commercial data, see, e.g., Courtney T. Ray and Debra L. Danisek, *Privacy Impact Assessment for the CBP License Plate Reader Technology*, DHS/CBP/IA-049(a), DHS Privacy Office, July 6, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp049a-cbplprtechnology-july2020.pdf (describing access to license plate data from private broker Vigilant Solutions). License plate data also comes from state departments of motor vehicles and the Drug Enforcement Administration. In addition, as of 2017, ATS was testing whether to ingest "commercially available social media information." Jonathan R. Cantor, *Privacy Impact Assessment Update for the Automated Targeting System*, DHS/CBP/PIA-006(e), DHS Privacy Office, January 13, 2017 (hereinafter *PIA Update for ATS*), 103, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-006-e-ats-january2017.pdf. For a full list of DHS and CBP systems from which ATS draws data in real time, see Privacy Office, *2019 Data Mining Report*, 19.

121 AFI, which appears to be directed primarily at non-Americans, helps CBP construct networks of associations by identifying "non-obvious relationships" and offers a variety of analytical tools along with a "platform for the research, collaboration, approval, and publication of [CBP's] finished intelligence products." Jonathan R. Cantor, *Privacy Impact Assessment Update for the Analytical Framework for Intelligence (AFI)*, DHS/CBP/PIA-010(a), DHS Privacy Office, September 1, 2016 (hereinafter *PIA Update for AFI*), 10, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp010a-afi-august2021.pdf. See also Privacy Office, *2019 Data Mining Report*, 33.

122 See Jonathan R. Cantor, *Privacy Impact Assessment for the TECS System: Platform*, DHS/CBP/PIA-021, DHS Privacy Office, August 12, 2016, 2, https://www.dhs.gov/sites/default/files/publications/DHS-PIA-ALL-021%20TECS%20System%20Platform.pdf.

123 Mary Ellen Callahan, *Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)*, DHS Privacy Office, June 1, 2012, 3, https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf. See also Spencer Woodman, "Documents Suggest Palantir Could Help Power Trump's 'Extreme Vetting' of Immigrants," *Verge*, December 21, 2016, https://www.theverge.com/2016/12/21/14012534/palantir-peter-thiel-trump-immigrant-extreme-vetting. AFI has added access to a number of ICE and law enforcement data sources since it was first launched. Cantor, *PIA Update for AFI*, 11.

124 Cantor, *PIA Update for AFI*, 4. AFI is also susceptible to relying on out-of-date information because it ingests databases in their entirety and there may be a lag in receiving updates from the source systems. Cantor, *PIA Update for AFI*, 1–4, 17, 18.

125 Debra L. Danisek, *Privacy Impact Assessment for the U.S. Customs and Border Protection Unified Secondary*, DHS/CBP/PIA-067, DHS Privacy Office, December 16, 2020, 1, 29–33, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp067-unifiedsecondary-june2021.pdf.

126 Cantor, *PIA Update for AFI*, 10. These include U.S. Citizenship and Immigration Services' Fraud Detection and National Security Directorate; ICE's Homeland Security Investigations Office of Intelligence; personnel in TSA's Office of Intelligence and Analysis; and DHS's Office of Intelligence and Analysis, among others.

127 Cantor, *PIA Update for AFI*, 15.

128 Elhady v. Piehota, No. 1:16-cv-00375-AJT-JFA (E.D. Va., filed Apr. 5, 2016), https://www.clearinghouse.net/chDocs/public/NS-VA-0008-0001.pdf (complaint for injunctive and declaratory relief).

129 The judge did not decide on the appropriate remedy, and before the case could proceed to develop solutions, it was appealed to the Fourth Circuit. Elhady v. Kable, 391 F. Supp. 3d 562, 577 (E.D. Va. 2019), *appeal docketed*, No. 20-1119 (4th Cir. Feb. 3, 2020).

130 Elhady v. Kable, 993 F. 3d 208 (4th Cir. 2021).

131 El Ali v. Barr, No. 8:18-cv-02415-PX (D. Md., filed Aug. 8, 2018).

132 El Ali v. Barr, 473 F. Supp. 3d 479 (D. Md. 2020), https://www.cair.com/wp-content/uploads/2020/07/ELALI.pdf.

133 ACLU, "Chebli v. Kable: Lawsuit Challenging Placement on No Fly List," last updated May 12, 2021, https://www.aclu.org/cases/chebli-v-kable-lawsuit-challenging-placement-no-fly-list.

134 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 Stelling, "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.

135 Stelling, "Border Is a Back Door."

136 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. The risk of misuse of TECS is magnified by the dearth of guidance or restrictions on using lookouts; the only written guidance dates to 1990, 13 years before DHS opened its doors. OIG, *CBP Targeted Americans*, 5.

137 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.

138 Winter, "Operation Whistle Pig."

139 See Patel et al., *Social Media Monitoring*, 8; Cantor, *PIA Update for ATS*, 33 (regarding sharing with Secure Flight); and Cantor, *PIA Update for AFI*, 2–3, 6. Data from the system can be shared under some circumstances with local, state, federal, and tribal law enforcement agencies, as well as with foreign governments and federal and foreign intelligence and counterterrorism agencies. Cantor, *PIA Update for ATS*, 57. For the Silent Partner and Quiet Skies systems, data from both lists may be shared within DHS and disseminated to the DOJ. Jonathan R. Cantor, Privacy Impact Assessment Update for Secure Flight, Silent Partner and Quiet Skies, DHS/TSA/PIA-018(i), DHS Privacy Office, April 19, 2019 (hereinafter *PIA Update for SPQS*), 10, https://www.dhs.gov/sites/default/files/publications/pia-tsa-spqs018i-april2019_1.pdf.

140 Records about an individual's presence on the Silent Partner list are kept in active status for seven years and dormant status for an additional eight; records showing that someone was selected for enhanced screening under either program are kept for seven years in TSA's Secure Flight system. Cantor, *PIA Update for SPQS*, 2–3.

141 TSA watch list master files are kept for 30 years after the date of entry of an individual's information. Jonathan R. Cantor, *Privacy Impact Assessment Update for Secure Flight*, DHS/TSA/PIA-018(h), DHS Privacy Office, July 12, 2017, 9, https://www.dhs.gov/sites/default/files/publications/pia_tsa_secureflight_18%28h%29_july2017.pdf.

142 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*), 14, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf.

143 ATS keeps data for up to 15 years even when the source system has a much shorter retention period. Privacy Office, *2015 Data Mining Report to Congress*, DHS, February 2016, 26, https://www.dhs.gov/sites/default/files/publications/2015%20Data%20Mining%20Report%20FINAL.pdf.

144 Privacy Office, *2019 Data Mining Report*, 24–25.

145 Civil Rights Litigation Clearinghouse, "Ibrahim v. Department of Homeland Security," University of Michigan Law School, accessed December 17, 2021, https://www.clearinghouse.net/detail.php?id=13632; and Ibrahim v. Department of Homeland Security, No. C 06-00545-WHA (N.D. Cal. 2006). See also Cantor, *PIA Update for AFI*, 2–3, 14 (reporting that the AFI's structure, in which the system stores multiple copies of the underlying data sources from which it draws, "poses significant privacy concerns" because of the "continuous replication of data," making it more likely that the system will end up with inaccurate or out-of-date information).

146 See Maura Dolan, "Appeals Court Rebukes Federal Government in 'No-Fly' Case, Ruling It Owes Millions in Legal Fees," *Los Angeles Times*, January 2, 2019, https://www.latimes.com/local/lanow/la-me-ln-no-fly-terrorist-9thcircuit-20190102-story.html; "The FBI Checked the Wrong Box and a Woman Ended Up on the Terrorism Watch List for Years," ProPublica, December 15, 2015, https://www.propublica.org/article/fbi-checked-wrong-box-rahinah-ibrahim-terrorism-watch-list; and Dan Levine, "FBI's No-Fly List Mistake Kicked Off Woman's Odyssey, Filing Says," Reuters, February 6, 2014, https://www.reuters.com/article/usa-nofly-ruling-idUSL2N-0LB20Z20140206.

147 Electronic Frontier Foundation, "Comments of the Electronic Frontier Foundation Regarding Notice of Proposed Rulemaking on the Collection and Use of Biometrics by U.S. Citizenship and Immigration Service, USCIS Docket No. USCIS–2019–0007, 85 Fed. Reg. 56,338," October 13, 2020, https://www.eff.org/files/2020/10/22/2020-10-13_-_dhs_nprm_on_biometric_collection_-_eff_website.pdf; and Jennifer Lynch, "Hart: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' 'Non-Obvious Relationships,'" Electronic Frontier Foundation, June 7, 2018, https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.

148 The department's data mining reports often have a more narrative and inclusive approach, but they are not comprehensive. As described in section III of this report, privacy impact assessments have a fairly narrow focus, covering individual data systems rather than painting a complete picture of DHS's handling and exploitation of travelers' data.

149 Karen Neuman, *Privacy Impact Assessment Update for the Automated Targeting System — TSA/CBP Common Operating Picture Phase II*, DHS/CBP/Pia-006(D), DHS Privacy Office, September 16, 2014, https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_tsacop_09162014.pdf. See also Cantor, *PIA Update for SPQS*, 2 (regarding the scope of individuals covered by risk assessment programs).

150 Jana Winter and Cora Currier, "Exclusive: TSA's Secret Behavior Checklist to Spot Terrorists," *Intercept*, March 27, 2015, https://theintercept.com/2015/03/27/revealed-tsas-closely-held-behavior-checklist-spot-terrorists.

151 See Brennan Center for Justice, "ICE Extreme Vetting Initiative: A Resource Page," November 16, 2017, https://www.brennancenter.org/our-work/research-reports/ice-extreme-vetting-initiative-resource-page.

152 Executive Order 13,769 of January 27, 2017, "Protecting the Nation from Foreign Terrorist Entry into the United States," 82 Fed. Reg. 8977, https://www.govinfo.gov/content/pkg/FR-2017-02-01/pdf/FR-2017-02-01.pdf; Immigration and Customs Enforcement, "Extreme Vetting Initiative: Statement of Objectives (SOO)," DHS, June 12, 2017, https://www.brennancenter.org/sites/default/files/Extreme%20Vetting%20Initiate%20-%20Statement%20of%20Objectives.pdf; and Homeland Security Investigations, "Attachment 2-Background," ICE-HSI-Data Analysis Service: Solicitation Number HSCE-MD-17-R-0010, Immigration and Customs Enforcement, DHS, June 12, 2017, https://web.archive.org/web/20180312231420/https://www.fbo.gov/?s=opportunity&mode=form&tab=core&id=ee93bc-c8a389d539fd9b927ec53dd2be&_cview=0.

153 Brennan Center for Justice et al. to Elaine C. Duke, acting secretary of homeland security, November 16, 2017, https://www.brennancenter.org/sites/default/files/Coalition%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%2011.15.17.pdf.

154 Hal Abelson et al. to Elaine C. Duke, acting secretary of homeland security, November 16, 2017, https://www.brennancenter.org/sites/default/files/Technology%20Experts%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%2011.15.17.pdf.

155 Thomas D. Homan, acting director of ICE, letter to the Honorable Kathleen M. Rice, ranking member of the H. Comm. on Homeland Security Subcomm. on Counterterrorism and Intelligence, ICE, April 25, 2018, https://www.brennancenter.org/sites/default/files/ICE%20Homan%20letter%20to%20Rice%20-%2004.25.18.pdf; and Blanket Purchase Agreement for General Dynamics Information Technology, Inc. from the Department of Homeland

Security, March 30, 2019, USASpending.gov, https://www.usaspending.gov/award/81011540.

156 Malaika Fraley, "The Public Has a Right to Know How DHS Is Spending Millions to Spy on Immigrants on Social Media," Electronic Frontier Foundation, March 28, 2022, https://www.eff.org/deeplinks/2022/03/public-has-right-know-how-dhs-spending-millions-spy-immigrants-social-media.

157 OIG, *Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted)*, DHS, May 2013 (hereinafter *TSA's SPOT*), 3, https://www.oig.dhs.gov/reports/2013-05/transportation-security-administrations-screening-passengers-observation-techniques. See also Mary Ellen Callahan, *Privacy Impact Assessment Update for the Screening of Passengers by Observation Techniques (SPOT) Program*, DHS/TSA/PIA-016(A), DHS Privacy Office, August 5, 2011, 2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-spot-update_0.pdf.

158 OIG, *Verification Review of Transportation Security Administration's Screening of Passengers by Observation Techniques/Behavior Detection and Analysis Program*, DHS, July 8, 2016 (hereinafter *Verification Review of SPOT*), 2, https://www.oig.dhs.gov/sites/default/files/assets/VR/FY16/OIG-16-111-VR-Jul16.pdf.

159 GAO, *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, May 20, 2010, 2, https://www.gao.gov/assets/gao-10-763.pdf. DHS's plans to validate SPOT after implementation were deemed deficient as well. GAO, *Aviation Security: Efforts to Validate*, 20.

160 In addition, the program did not have a "comprehensive training program" or a financial plan, and also did not "ensure outreach" to partners such as law enforcement agencies. OIG, *TSA's SPOT*, 1, 9.

161 GAO, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, November 2013, https://www.gao.gov/assets/gao-14-159.pdf; and GAO, *Aviation Security: Efforts to Validate*, 60.

162 OIG, *Verification Review of SPOT*, 1, 2; and OIG, *TSA's SPOT*.

163 GAO, "Aviation Security: TSA Does Not Have Valid Evidence Supporting Most of the Revised Behavioral Indicators Used in Its Behavior Detection Activities," July 20, 2017, 1, https://www.gao.gov/products/gao-17-608r.

164 Michael S. Schmidt and Eric Lichtblau, "Racial Profiling Rife at Airport, U.S. Officers Say," *New York Times*, August 11, 2012, https://www.nytimes.com/2012/08/12/us/racial-profiling-at-boston-airport-officials-say.html.

165 Schmidt and Lichtblau, "Racial Profiling Rife." See also Rep. Bennie Thompson to John S. Pistole, TSA administrator, June 21, 2011, https://homeland.house.gov/imo/media/doc/20110621171505-44153.pdf; *TSA's SPOT Program and Initial Lessons from the LAX Shooting, Hearing Before the Subcomm. on Transportation Security of the H. Comm. on Homeland Security*, 113th Cong. (2013), https://www.govinfo.gov/content/pkg/CHRG-113hhrg87373/html/CHRG-113hhrg87373.htm; and Joe Davidson, "Lawmaker Challenges TSA on Claims of Ethnic Profiling," *Washington Post*, November 28, 2011, https://www.washingtonpost.com/politics/lawmaker-challenges-tsa-on-claims-of-ethnic-profiling/2011/11/28/gIQAtOiO6N_story.html.

166 GAO, *Aviation Security: TSA Has Policies That Prohibit Unlawful Profiling but Should Improve Its Oversight of Behavior Detection Activities*, April 2019, 18, https://www.gao.gov/assets/gao-19-268.pdf; Davidson, "Lawmaker Challenges TSA"; and Janet Napolitano, secretary of homeland security, memorandum, "The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities," April 26, 2013 (hereinafter "DHS's Commitment to Nondiscriminatory Law Enforcement"), 1, https://www.dhs.gov/sites/default/files/publications/secretary-memo-race-neutrality-2013_0.pdf.

167 GAO, *Aviation Security: TSA Has Policies That Prohibit Unlawful Profiling*, 7 (noting that "in early fiscal year 2018, TSA ended the stand-alone behavior detection program and eliminated the behavior detection officer position. TSA also began integrating the former behavior detection officers into the screener workforce. . . ."); Christopher Muther, "How Decades of Security Blunders Led to the Formation of the TSA and Forever Changed the Way We Fly," *Boston Globe*, updated September 24, 2021, https://www.bostonglobe.com/2021/09/24/lifestyle/how-decades-security-blunders-led-formation-tsa-forever-changed-way-we-fly; and Kylie Bielby, "GAO: TSA Should Better Target Unlawful Profiling," *Homeland Security Today*, June 4, 2019, https://www.hstoday.us/subject-matter-areas/airport-aviation-security/gao-tsa-should-better-target-unlawful-profiling (noting that in "August 2017, TSA began training screeners on its new behavioral indicators").

168 Peter Pietra and Hugo Teufel III, *Privacy Impact Assessment for the Screening of Passengers by Observation Techniques (SPOT) Program*, DHS, August 5, 2008, 6–7, https://www.dhs.gov/sites/default/files/publications/privacy_pia_tsa_spot_0.pdf (noting that electronic records in the SPOT database are kept for 15 years, while encounters resulting in incident reports are kept for anywhere from 3 to 25 years, depending on the system. If they were entered into TECS or ATS, their retention would be governed by those systems' policies, which provide for preservation for up to 75 and 15 years, respectively). Privacy Office, "DHS/CBP/PIA-006 Automated Targeting System." See also Callahan, *PIA for TECS*; and OIG, *Summary Report: Persistent Data Issues Hinder DHS Mission, Programs, and Operations*, DHS, May 24, 2021, 2, https://www.oig.dhs.gov/sites/default/files/assets/2021-05/OIG-21-37-May21.pdf.

169 Privacy Office, *2019 Data Mining Report*, 27 (noting that the programs are designed to "address unknown and partially identified threats" through "risk-based, intelligence-driven rules"). On December 25, 2009, Umar Farouk Abdulmutallab smuggled a bomb on board a Northwest Airlines flight from Amsterdam in his underwear, which he attempted to detonate as the plane descended toward Detroit. The resulting explosion caused a fire but no major injuries, and the plane landed safely. Abdulmutallab was sentenced to life in prison in February 2012. Jason Ryan, "Underwear Bomber Abdulmutallab: 'Proud to Kill in the Name of God,'" ABC News, February 16, 2012, https://abcnews.go.com/Blotter/underwear-bomber-abdulmutallab-sentenced-life-prison/story?id=15681576.

170 Cantor, *PIA Update for SPQS*, 1.

171 The program was apparently started in 2012 but ramped up in March 2018. OIG, *TSA Needs to Improve Management of the Quiet Skies Program (Redacted)*, DHS, November 25, 2020, 2, 6, https://www.oig.dhs.gov/sites/default/files/assets/2020-11/OIG-21-11-Nov20-Redacted.pdf; and Cantor, *PIA Update for SPQS*, 1, 6 (describing the process of determining matches to a TSA "targeting rule"). These individuals are not among those listed in the TSDB.

172 Cantor, *PIA Update for SPQS*, 2, 6; and Jana Winter, "Welcome to the 'Quiet Skies,'" *Boston Globe*, July 28, 2018, https://www.bostonglobe.com/metro/2018/07/28/welcome-the-quiet-skies-air-marshals-track-ordinary-travelers-like-terror-suspects-controversial-new-surveillance-program/uEvS2VJ2n3DHfFfPJ4z7DJ/story.html. The utility of deploying federal air marshals on flights had been the subject of serious questioning prior to Quiet Skies, with the DHS inspector general determining that the Federal Air Marshal Service "lacked performance measures and budget data to show its contributions and cost-effectiveness to address aviation transportation security risks." OIG, *TSA Needs to Improve Management of the Quiet Skies Program*, 28.

173 Jana Winter, "TSA Admits 'Quiet Skies' Surveillance Snared Zero Threats," *Boston Globe*, August 2, 2018, https://www.bostonglobe.com/metro/2018/08/02/tsa-says-quiet-skies-surveillance-snared-zero-threats/dsCm4BG3pq8v3xhi01zhLI/story.html?p1=Article_Inline_Text_Link. Among those reported to have been targeted: a Virginia woman who had flown to Turkey for an arts-and-crafts course, a professional basketball player, a working flight attendant, a business executive, and a law enforcement officer

employed by another federal agency. Jana Winter, "TSA Says Air Marshals Don't Follow 'Ordinary' Travelers. Some Ordinary Travelers Beg to Differ," *Boston Globe*, August 18, 2018, https://www.bostonglobe.com/news/nation/2018/08/18/tsa-says-armed-air-marshals-don-follow-ordinary-fliers-some-ordinary-fliers-beg-differ/Y0k3mV3HPUCgzS20PpAU3H/story.html.

174 OIG, *TSA Needs to Improve Management of the Quiet Skies Program*, 3. OIG also documented other problems with Quiet Skies, including softwares glitches that resulted in people remaining on the list long after they were no longer considered a risk; the use of information obtained via Quiet Skies for purposes other than screening at checkpoints; and TSA's failure to obtain required approvals from the Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel, as well as its failure to update compliance documentation.

175 Cantor, *PIA Update for SPQS*, 2–3. See also Jana Winter and Jenn Abelson, "TSA Says It No Longer Tracks Regular Travelers as If They May Be Terrorists," December 15, 2018, https://www.bostonglobe.com/news/nation/2018/12/15/curtails-quiet-skies-passenger-surveillance/2lRAv2AwjGpUcgq08mHaPM/story.html.

176 Napolitano, "DHS's Commitment to Nondiscriminatory Law Enforcement," 1.

177 See DHS, "The Department of Homeland Security's Commitment to Race Neutrality in Law Enforcement Activities," June 1, 2004, https://www.dhs.gov/xlibrary/assets/training/xus/crcl/racelawofficers/Common/pdf/dhs_profiling_policy.pdf; and DOJ, "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies, June 2003, https://www.dhs.gov/xlibrary/assets/training/xus/crcl/racelawofficers/Common/pdf/doj_profiling_guidance.pdf.

178 CBP, "CBP Policy on Nondiscrimination in Law Enforcement and All Other Administered Programs," updated February 24, 2020, https://www.cbp.gov/about/eeo-diversity/policies/nondiscrimination-law-enforcement-activities-and-all-other-administered.

179 The policy permits the consideration of race and ethnicity when it is "specific to particular suspects or incidents or ongoing criminal activities, schemes or enterprises."

180 Legal information Institute of Cornell Law School, "Strict Scrutiny," accessed February 17, 2022, https://www.law.cornell.edu/wex/strict_scrutiny.

181 CBP, "CBP Policy on Nondiscrimination in Law Enforcement."

182 Napolitano, "DHS's Commitment to Nondiscriminatory Law Enforcement"; DHS, "Regulations Regarding Nondiscrimination on the Basis of Race, Color, or National Origin in Programs or Activities Receiving Federal Financial Assistance from the Department of Homeland Security; Interim Final Rule," March 6, 2003, https://www.justice.gov/sites/default/files/crt/legacy/2010/12/14/dhsvi.pdf; and CBP, "CBP Policy on Nondiscrimination in Law Enforcement."

183 See, e.g., Dalia Mogahed and Erum Ikramullah, *American Muslim Poll 2020: Amid Pandemic and Protest*, Institute for Social Policy and Understanding, October 1, 2020, https://www.ispu.org/american-muslim-poll-2020-amid-pandemic-and-protest; Michael T. Luongo, "Traveling While Muslim Complicates Air Travel," *New York Times*, November 7, 2016, https://www.nytimes.com/2016/11/08/business/traveling-while-muslim-complicates-air-travel.html; Amnesty International, *Threat and Humiliation: Racial Profiling, Domestic Security, and Human Rights in the United States*, 2004, 8, https://www.amnestyusa.org/pdfs/rp_report.pdf; and Memorandum and Order Granting in Part and Denying in Part Official-Capacity Defendants' Motion to Dismiss, Cherri v. Mueller, 951 F. Supp. 2d 918 (E.D. Mich. 2013), https://www.clearinghouse.net/chDocs/public/NS-MI-0001-0002.pdf.

184 Appendix, Motion for Summary Judgement, Ex. 18 at 2, *Cherri v. Mueller*, 951 F. Supp. 2d, https://www.brennancenter.org/sites/default/files/2022-01/Cherri%20v.%20Mueller%20Motion%20Sumary%20Judgement.pdf.

185 See U.S. Citizenship and Immigration Services, "Refugees and Asylum," accessed February 17, 2022, https://www.uscis.gov/humanitarian/refugees-asylum; and Department of State, "Temporary Religious Worker Visa," accessed February 17, 2022, https://travel.state.gov/content/travel/en/us-visas/other-visa-categories/temporary-religious-worker.html. See also U.S. Citizenship and Immigration Services, "Special Immigrant Religious Workers," updated January 25, 2022, https://www.uscis.gov/working-in-the-united-states/permanent-workers/employment-based-immigration-fourth-preference-eb-4/special-immigrant-religious-workers (non-minister special immigrant religious worker program).

186 Napolitano, "DHS's Commitment to Nondiscriminatory Law Enforcement," 1–2.

187 Napolitano, "DHS's Commitment to Nondiscriminatory Law Enforcement," 2.

188 Rachel L. Swarns, "Program's Value in Dispute as a Tool to Fight Terrorism," *New York Times*, December 21, 2004, https://www.nytimes.com/2004/12/21/us/programs-value-in-dispute-as-a-tool-to-fight-terrorism.html; and Chris Rickerd, "Homeland Security Suspends Ineffective, Discriminatory Immigration Program," ACLU, May 6, 2011, https://www.aclu.org/blog/speakeasy/homeland-security-suspends-ineffective-discriminatory-immigration-program.

189 Napolitano, "DHS's Commitment to Nondiscriminatory Law Enforcement," 2. CBP's policy seems to encourage its agents to use this authority, explicitly stating that agents can consider nationality on an individualized, discretionary basis as a "screening, investigation, or enforcement factor" with "no further justification." CBP, "CBP Policy on Nondiscrimination in Law Enforcement."

190 Zolan Kanno-Youngs, Mike Baker, and Mariel Padilla, "U.S. Stops Dozens of Iranian-Americans Returning from Canada," *New York Times*, January 5, 2020, https://www.nytimes.com/2020/01/05/us/politics/iranian-americans-border.html.

191 Patrick Grubb, "Source Provides Directive Telling CBP Officers to Detain Iranian-Born Travelers," *Northern Light*, January 29, 2020, https://www.thenorthernlight.com/stories/source-provides-directive-telling-cbp-officers-to-detain-iranian-born-travelers,9315; and Abigail Hauslohner and Nick Miroff, "U.S. Officials Investigating Document That Instructs Border Agents to Profile Iranians, Palestinians, and Lebanese," *Washington Post*, January 30, 2020, https://www.washingtonpost.com/immigration/us-officials-investigating-document-that-instructs-border-agents-to-profile-iranians-palestinians-and-lebanese/2020/01/30/2a92df40-438f-11ea-b5fc-eefa848cde99_story.html.

192 Rep. Suzan K. DelBene et al. to Mark A. Morgan, acting commissioner, CBP, January 6, 2020, https://delbene.house.gov/uploadedfiles/skd_iranian_detention_letter_-_with_signature_pages.pdf; Office of Rep. Suzan K. DelBene, "DelBene Continues to Demand Answers from CBP on Iranian Detentions at Border," press release, August 21, 2020, https://delbene.house.gov/news/documentsingle.aspx?DocumentID=2648; Grace McCarthy, "U.S. Lawmakers Have Yet to Receive CBP Apology for Iranian-American Detention, DelBene Says," *Northern Light*," February 9, 2022, https://www.thenorthernlight.com/stories/no-cbp-apology-for-january-2020-border-detention-delbene-says,19077; and Patrick Grubb, "Border Crackdown on Iranian Travelers Was a Local Initiative, CBP Whistleblower Says," *Northern Light*, January 22, 2020, https://www.thenorthernlight.com/stories/border-crackdown-on-iranian-travelers-was-a-local-initiative-cbp-whistleblower-says,9255.

193 CBP, "CBP Policy on Nondiscrimination in Law Enforcement."

194 Napolitano, "DHS's Commitment to Nondiscriminatory Law Enforcement."

195 Notably, while the incident followed tensions between Iran and the United States after a U.S. drone strike killed Qassem Soleimani, a general in Iran's Islamic Revolutionary Guard Corps, prompting a threat of retaliation from Iran, DHS acknowledged that it had "no information indicating a specific, credible threat" to the United States at the time. DHS, "Summary of Terrorism Threat to the U.S. Homeland," National Terrorism Advisory System Bulletin, January 4, 2020,

https://www.dhs.gov/sites/default/files/ntas/alerts/20_0104_ntas_bulletin.pdf.

196 Although the need to consolidate congressional oversight of DHS has long been recognized, it has not yet led to substantial changes. See Carrie Cordero, *Reforming the Department of Homeland Security Through Enhanced Oversight and Accountability*, Center for a New American Security, May 12, 2020 (hereinafter *Reforming the DHS*), https://www.cnas.org/publications/reports/reforming-the-department-of-homeland-security-through-enhanced-oversight-accountability; and Aspen Institute, *Task Force Report on Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security*, September 2013, https://cdn.annenbergpublicpolicycenter.org/Downloads/Sunnylands/homeland%20security%20report%2009-11-13.pdf.

197 DHS Reform Act of 2020, H.R. 8791, 116th Cong. (2020).

198 House Committee on Homeland Security, "Committee Advances Slate of 12 Bipartisan Homeland Security Bills," press release, October 26, 2021, https://homeland.house.gov/news/legislation/committee-advances-slate-of-12-bipartisan-homeland-security-bills; Department of Homeland Security Inspector General Transparency Act, H.R. 5633, 117th Cong. (2021); and Department of Homeland Security Office for Civil Rights and Civil Liberties Authorization Act, H.R. 4349, 117th Cong. (2021).

199 In FY 2019, for example, Congress appropriated more than $25 million for CRCL, above the White House's $21 million budget request. Department of Homeland Security Appropriations Bill, H. Rept. 115-948, 115th Cong. (2019). The same pattern has held for more recent budgets: in FY 2021, Congress appropriated more than $34 million for CRCL, nearly $10 million above what was requested. DHS, *Department of Homeland Security Office of the Secretary and Executive Management: Budget Overview, Fiscal Year 2021 Congressional Justification,* February 9, 2020, 73, https://www.dhs.gov/sites/default/files/publications/office_of_the_secretary_and_executive_management.pdf; and DHS, *Department of Homeland Security Office of the Secretary and Executive Management: Budget Overview, Fiscal Year 2022 Congressional Justification,* May 26, 2021, 71, https://www.dhs.gov/sites/default/files/publications/office_of_the_secretary_and_executive_management_0.pdf.

200 Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 103, 705, 116 Stat. 2144, 2219 (codified as amended at 6 U.S.C. §§ 113, 345 (2004)) (charging CRCL with overseeing "compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department").

201 6 U.S.C. § 345 (2004) (directing the office to "ensure that the protection of civil rights and civil liberties is appropriately incorporated into Department programs and activities").

202 6 U.S.C. § 345 (2004).

203 6 U.S.C. § 345(b) (2004); 42 U.S.C. §2000ee–1(g) (2018); and CRCL, "Community Engagement," DHS, accessed February 23, 2022, https://www.dhs.gov/community-engagement.

204 42 U.S.C. § 2000ee–1 (2018).

205 Compare 6 U.S.C. § 345 (establishing officer for civil rights and civil liberties without conferring subpoena authority) with 6 U.S.C. §§ 142 (b)(1)(C) & (b)(2) (conferring subpoena authority on privacy officer). See also Kareem W. Shora, "A Twenty-Year Lesson: The Role of Civil Rights in Securing Our Nation," *Journal of National Security Law and Policy* 12 (2021): 191 ("The internal civil rights oversight office within the US Department of Homeland Security (DHS), for example, unlike similar offices such as the one at the US Department of the Interior, was not provided with the subpoena authorities needed to effectively conduct its oversight investigations. This has sometimes left the effectiveness of the office's oversight investigations to the whims of the component agencies being investigated.").

206 Scott Shuchart, *Building Meaningful Civil Rights and Liberties Oversight at the U.S. Department of Homeland Security*, Center for American Progress, April 2, 2019, 6, https://www.americanprogress.org/article/building-meaningful-civil-rights-liberties-oversight-u-s-department-homeland-security.

207 Shirin Sinnar, "Institutionalizing Rights in the National Security Executive," *Harvard Civil Rights-Civil Liberties Law Review* 50 (2015): 289–357, https://harvardcrcl.org/wp-content/uploads/sites/10/2015/11/Institutionalizing-Rights-in-the-National-Security-Executive.pdf.

208 Sinnar, "Institutionalizing Rights in the National Security Executive," 305.

209 Shuchart, *Building Meaningful Civil Rights and Liberties Oversight*, 1, 6.

210 Margo Schlanger, "Offices of Goodness: Influence Without Authority in Federal Agencies," *Cardozo Law Review* 36 (2018): 68–72, http://cardozolawreview.com/wp-content/uploads/2018/08/SCHLANGER.36.1.pdf.

211 See, e.g., Asian Law Caucus et al. to Janet Napolitano, secretary of homeland security, July 21, 2009, http://perma.cc/77HW-EQ9D (letter on behalf of 14 civil society organizations raising structural and other concerns with the functioning of the office); and Government Accountability Project to Rep. Elijah Cummings et al., June 27, 2019, https://www.whistleblower.org/wp-content/uploads/2019/06/Congressional-Letter-OIG-CRCL-Failures.pdf (citing CRCL's failure to adequately respond to multiple whistleblower allegations of detainee abuse and mistreatment).

212 *Working with Communities to Disrupt Terror Plots, Hearing Before the H. Comm. on Homeland Security Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment*, 111th Cong. (2010) (statement of Rep. Bennie G. Thompson), https://www.govinfo.gov/content/pkg/CHRG-111hhrg57457/html/CHRG-111hhrg57457.htm; and Sinnar, "Institutionalizing Rights in the National Security Executive," 304n59.

213 Thompson, *Working with Communities to Disrupt Terror Plots*.

214 Scott Shuchart, "Careless Cruelty: Civil Servants Said Separating Families Was Illegal. The Administration Ignored Us," *Washington Post*, October 25, 2018, https://www.washingtonpost.com/news/posteverything/wp/2018/10/25/feature/civil-servants-said-separating-families-was-illegal-the-administration-ignored-us.

215 In addition to I&A, other DHS components collect intelligence and circulate threat reports, but we have been unable to identify any publicly available policies that require such components to submit their intelligence reports to CRCL for review. CBP and TSA also have their own civil rights and civil liberties functions, while other components — including ICE, U.S. Citizenship and Immigration Services, and the Secret Service — have CRCL offices that appear to play exclusively an internal-facing function, focusing on employee diversity and equal employment matters. I&A has no internal CRCL office. A bill introduced in 2017 would have required every DHS component to appoint a career officer who would coordinate with CRCL, but the Senate did not take it up. DHS Authorization Act, H.R. 2825, 115th Cong. (2017); and S. Rep. 115-351, 115th Cong. (2018).

216 Federal Protective Service, "Civil Activists and Extremists Action Calendar (Protests, Demonstrations, Marches, and Special Events of Interest)," DHS, March 3, 2006, https://www.prisonlegalnews.org/media/publications/civil_activists_and_extremists_action_calendar_federal_protective_services_2006.pdf. According to a summary of CRCL's review provided to the ACLU, the office found that the Federal Protective Service had not abused its authority, although it had "failed to differentiate adequately between civil activist and violent extremist organizations." Robyn Greene, "DHS Concludes They Have Authority to Monitor Political Activities of Advocacy Groups," ACLU, March 7, 2011, https://www.aclu.org/blog/national-security/privacy-and-surveillance/dhs-concludes-they-have-authority-monitor-political.

217 George Joseph, "Exclusive: Feds Regularly Monitored Black

Lives Matter Since Ferguson," *Intercept*, July 24, 2015, https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson; and Federal Emergency Management Agency, "FEMA Regions I, II and III: Scheduled Protest for April 30–May 3," DHS, April 2015, https://www.documentcloud.org/documents/2178937-4-2015-4-30-5-3-fema-protest-report-includes.html.

218 Joseph, "Feds Regularly Monitored Black Lives Matter"; and Jason Leopold, "Emails Show Feds Have Monitored 'Professional Protester' DeRay Mckesson," *VICE*, August 11, 2015, https://www.vice.com/en/article/qv58n3/emails-show-feds-have-monitored-professional-protester-deray-mckesson.

219 Jimmy Tobias, "Exclusive: ICE Has Kept Tabs on 'Anti-Trump' Protesters in New York City," *Nation*, March 6, 2019, https://www.thenation.com/article/archive/ice-immigration-protest-spreadsheet-tracking.

220 Immigration and Customs Enforcement, "ICE Significant Incident Report on Vigil for Jean Carlos Jiménez-Joseph," DHS, May 27, 2017, https://www.documentcloud.org/documents/20892417-ice-significant-incident-report-on-vigil-for-jean-jiminez-joseph.

221 José Olivares and John Washington, "ICE Discussed Punishing Immigrant Advocates for Peaceful Protests," *Intercept*, June 17, 2021, https://theintercept.com/2021/06/17/ice-retaliate-immigrant-advocates-surveillance.

222 Immigrant Rights Voices, accessed December 16, 2021, https://www.immigrantrightsvoices.org/#.

223 See *FY2010 Budget Request, Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 111th Cong. (2009) (testimony of Bart R. Johnson, undersecretary, I&A), https://www.dhs.gov/news/2009/06/24/acting-under-secretary-bart-r-johnsons-testimony-fy-2010-budget-request-office (noting that DHS had put in place an "interim clearance process," which "established mandatory review and concurrence" by CRCL, the Privacy Office, DHS's general counsel, and I&A's Intelligence Oversight Section, with disagreements elevated to the deputy secretary for a final decision); and I&A, *DHS Intelligence and Analysis Review and Clearance of Analytic Products Disseminated Outside the Federal Government*, DHS, April 9, 2013, 2, https://s3.documentcloud.org/documents/7034402/2013-IA-901.pdf.

224 For a discussion of the evolution of this policy, see Tia Sewell and Benjamin Wittes, "The Evolution of DHS Intelligence Review Policy," *Lawfare* (blog), August 14, 2020, https://www.lawfareblog.com/evolution-dhs-intelligence-review-policy.

225 See notes 48–49 and accompanying text.

226 Schlanger, "Offices of Goodness," 96. Schlanger explains the pros and cons of different types of reviews, suggesting that reviews that are triggered by recognition of a problem or by an important stakeholder and are potentially public provide the most opportunities for impact.

227 CRCL, "Civil Rights and Civil Liberties Completed Impact Assessments and Related Documents," DHS, accessed December 21, 2021, https://www.dhs.gov/publication/civil-rights-civil-liberties-completed-impact-assessments-and-related-documents (listing eight assessments and one follow-up).

228 Timothy J. Keefer, *Civil Liberties Impact Assessment for the Screening of Passengers by Observation Techniques (SPOT) Program*, DHS CRCL, March 5, 2009 (hereinafter *CRCL Impact Assessment for the SPOT Program*), https://www.aclu.org/sites/default/files/field_document/March-5-2009-Civil-Liberties-Impact-Assessment-for-the-SPOT-Program-007857-007880-LR.pdf.

229 Sinnar, "Institutionalizing Rights in the National Security Executive," 330n208.

230 42 U.S.C. § 2000ee–1(a)(4) (2018). As part of the office's statutory role to provide advice to the secretary regarding "proposals to retain or enhance a particular governmental power," the office is specifically directed to consider whether "the need for the power is balanced with the need to protect privacy and civil liberties."

231 Keefer, *CRCL Impact Assessment for the SPOT Program*, 3n3.

232 GAO, *Aviation Security: TSA Should Limit Future Funding*, 47.

233 Schmidt and Lichtblau, "Racial Profiling Rife at Airport."

234 The assessment, which took almost two years to complete, was ordered by Secretary of Homeland Security Janet Napolitano in response to public and congressional concerns about these searches. Margo Schlanger, *Civil Rights/Civil Liberties Impact Assessment: Border Searches of Electronic Devices*, DHS CRCL, December 29, 2011 (hereinafter Schlanger, *CRCL Impact Assessment: Border Searches of Electronic Devices*), 12, https://www.dhs.gov/sites/default/files/publications/crcl-border-search-impact-assessment_06-03-13_1.pdf.

235 There is currently a circuit split on whether extensive electronic border searches require any type of suspicion, which the Supreme Court has declined to address. Merchant v. Mayorkas, 988 F. 3d 8 (1st Cir. 2021), *cert. denied*, 594 U.S. ___ (2021). See also *Merchant v. Mayorkas*, 988 F. 3d 8 (holding that "border agents may review the material stored on international travelers' devices without a warrant, probable cause, or even reasonable suspicion" and need not limit examination to searches for contraband, but may "search for evidence of any possible violation of . . . laws that customs and immigration agencies help enforce"); U.S. v. Cano, 934 F. 3d 1002 (9th Cir. 2019) (holding that the border search exception "authorizes warrantless searches of a cell phone only to determine whether the phone contains contraband" and that forensic searches require reasonable suspicion); and U.S. v. Touset, 890 F. 3d 1227 (11th Cir. 2018) (observing that there was "no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property").

236 Tamara Kessler, *Civil Rights/Civil Liberties Impact Assessment: Border Searches of Electronic Devices*, DHS CRCL, January 29, 2013 (hereinafter Kessler, *CRCL Impact Assessment: Border Searches of Electronic Devices*), 2, https://www.dhs.gov/sites/default/files/publications/crcl-border-search-impact-assessment_01-29-13_1.pdf.

237 Sinnar, "Institutionalizing Rights in the National Security Executive," 306.

238 CRCL did recommend some safeguards, including that CBP agents should record a reason for their searches, collect data on the distribution of electronic device searches by race and ethnicity of travelers, and remedy any disparate impact, and that travelers subjected to electronic searches be referred to a redress program. Schlanger, *CRCL Impact Assessment: Border Searches of Electronic Devices*. CRCL's 2013 follow-up essentially found that CBP had complied with all of the office's recommendations and concluded that its review of two years' worth of searches showed no ethnic bias, though the searches subject to review were defined to exclude those related to watch lists. Kessler, *CRCL Impact Assessment: Border Searches of Electronic Devices*. As discussed in section II under "DHS Data Collection," subsequent OIG reports released in 2018 and 2021 have panned CBP for poor oversight over these searches, including officers' failure to properly document them. OIG, *CBP's Searches of Electronic Devices*; and OIG, *CBP Continues to Experience Challenges*.

239 Tamara Kessler, *Civil Rights/Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers*, DHS CRCL, March 1, 2013, ii, https://www.dhs.gov/sites/default/files/publications/DHS%20Support%20to%20National%20Network_0_0.pdf.

240 Kessler, *CRCL Impact Assessment: DHS Support to the National Network of Fusion Centers*, 4–5.

241 6 U.S.C. § 345(a)(6) (2004).

242 CRCL, *Semiannual Report to Congress: First and Second Quarters, FY 2021 (October 1, 2020–March 30, 2021)*, DHS, November 8, 2021, 10–11, https://www.dhs.gov/sites/default/files/2021-12/

fy-21-q1-q2-semiannual-report.pdf. The inspector general's office typically retains fewer than 30 complaints a year, and 5–10 percent of complaints are referred to the components. CRCL, "CRCL Annual Reports to Congress," DHS, accessed December 16, 2021, https://www.dhs.gov/publication/crcl-annual-reports.

243 6 U.S.C. § 345 (2004); 42 U.S.C. § 2000ee–1 (2018); and Schlanger, *CRCL Impact Assessment: Border Searches of Electronic Devices*, 4.

244 CRCL, *Fiscal Year 2014 Annual Report to Congress*, DHS, July 28, 2015, 24, https://www.dhs.gov/sites/default/files/publications/crcl-fy-2014-annual-report_0.pdf; CRCL, *Semiannual Report to Congress: First and Second Quarters, FY 2020 (October 1, 2019–March 31, 2020)*, DHS, January 8, 2021, 12–13, https://www.dhs.gov/sites/default/files/publications/fy-20-q1-q2-semiannual-report.pdf; and CRCL, *Semiannual Report to Congress: Third and Fourth Quarters, FY 2020 (April 1, 2020–September 30, 2020)*, DHS, August 13, 2021, 12–13, https://www.dhs.gov/sites/default/files/publications/crcl-fy-20-q3-q4-semiannual-report-508.pdf. Since the office does not open an investigation on every complaint it receives, the actual number of complaints is higher.

245 CRCL, *Fiscal Year 2019 Annual Report to Congress*, DHS, August 5, 2021, 28, https://www.dhs.gov/sites/default/files/publications/crcl-fy-2019-annual-report_0.pdf.

246 Schlanger, *CRCL Impact Assessment: Border Searches of Electronic Devices*, 19–20.

247 The report must include a summary of "the type of advice provided and the response given to such advice" and "a summary of the disposition of . . . complaints, the reviews and inquiries conducted, and the impact of the activities of such officer." 42 U.S.C. § 2000ee–1(f)(2) (2018). The secretary of homeland security is also required to file an annual congressional report "detailing any allegations of [civil rights or civil liberties] abuses . . . and any actions taken by the Department in response to such allegations." 6 U.S.C. § 345 (2004).

248 Shuchart, *Building Meaningful Civil Rights and Liberties Oversight*, 12. See also Margo Schlanger, "Increasing the Internal Influence of Civil Rights Offices: Written Testimony for the U.S. Commission on Civil Rights," November 2, 2018, 3, https://securisync.intermedia.net/us2/s/folder?public_share=PLLIdLtEW4WTVW-6mzucmuh0011ef58&id=L1BhbmVsIDQvTWFyZ28gU2NobGFuZ2Vy.

249 CRCL, "CRCL Recommendation and Investigation Memos," accessed December 17, 2021, https://www.dhs.gov/publications-library/collections/crcl-recommendation-and-investigation-memos.

250 See, e.g., CRCL, "Questioning Advocates and Journalists at the Lukeville, Arizona and San Ysidro, California Ports of Entry," DHS, December 6, 2019, https://www.dhs.gov/sites/default/files/publications/retention-memo-cbp-questioning-advocates-journalists-at-poe-12-06-19.pdf; and Katherine Culliton-González, officer, CRCL, and Susan Mathias, assistant general counsel, DHS Office of the General Counsel, to Troy Miller, acting commissioner, CBP, et al., "Recommendation Memo Related to the Implementation of Migrant Protection Protocols," memorandum, January 29, 2021, https://www.dhs.gov/sites/default/files/publications/mpp-redacted-recommendation-memo-01-29-21.pdf.

251 6 U.S.C. § 142 (2007).

252 OIG, *Summary Report: Persistent Data Issues*, 2.

253 6 U.S.C. § 142 (2007). See also DHS, "Delegation to the Chief Privacy Officer/Chief Freedom of Information Act Officer," June 2, 2020, https://www.dhs.gov/sites/default/files/publications/13001_revision_1_-_cpo_delegation_issued_06-02-2020.pdf.

254 Privacy Office, *OIG Privacy Incident Report and Assessment*, DHS, February 2011, https://www.dhs.gov/sites/default/files/publications/priv-oig-privacy-incident-report-assessment-022011.pdf.

255 OIG, *DHS Privacy Office Needs to Improve Oversight of Department-Wide Activities, Programs, and Initiatives*, DHS, November 4, 2020, 3, https://www.oig.dhs.gov/sites/default/files/assets/2020-12/OIG-21-06-Nov20.pdf.

256 OIG, *DHS Privacy Office Needs to Improve Oversight*, 15.

257 DHS, "DHS Instruction 047-01-005: Component Privacy Officer," February 6, 2017, 1, https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf.

258 These include annual reports to Congress. Privacy Office, "Privacy Office Annual Reports," DHS, accessed December 17, 2021, https://www.dhs.gov/publication/privacy-office-annual-reports. Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 requires semiannual reports. DHS, "DHS Section 803 Reports to Congress," accessed December 17, 2021, https://www.dhs.gov/publication/dhs-section-803-reports-congress. The Federal Agency Data Mining Reporting Act of 2007 requires an additional set of annual reports detailing its programs that use data mining capabilities. Privacy Office, "DHS Data Mining Reports," DHS, accessed December 17, 2021, https://www.dhs.gov/publication/dhs-data-mining-reports.

259 The statute provides that the privacy officer shall submit independent reports to Congress "without any prior comment or amendment by the Secretary, Deputy Secretary, or any other officer or employee of the Department or the Office of Management and Budget [OMB]." See 6 U.S.C. § 142(e)(1) (2007). The DOJ Office of Legal Counsel has taken the position that both the secretary of homeland security and OMB must be permitted to review and submit comments on the privacy officer's reports, although the privacy officer need not edit reports in response to those comments. *Constitutionality of the Direct Reporting Requirement in Section 802(e)(1) of the Implementing Recommendations of the 9/11 Commission Act of 2007*, 32, Op. O.L.C. 27, 31 (2008). Accordingly, although the privacy officer has reportedly submitted reports to OMB for review since 2008, its statutory authority to submit reports that do not reflect the views of OMB — even if accompanied by OMB's comments — is a significant grant of independence.

260 Privacy Act of 1974, 5 U.S.C. § 552(a)(e); and DHS, "System of Records Notices (SORNs)," accessed December 21, 2021, https://www.dhs.gov/system-records-notices-sorns. DHS has not always been punctual in its release of disclosures required by the Privacy Act and other statutes. For example, a DHS component published a SORN related to certain social media monitoring and situational awareness activities five years after the directive regarding such activities was first issued — and a related PIA two years after that — highlighting its apparent failure to be in timely compliance with statutory obligations. Jonathan R. Cantor, *Privacy Impact Assessment for the Publicly Available Social Media Monitoring and Situational Awareness Initiative*, DHS Privacy Office, March 25, 2019, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp58-socialmedia-march2019.pdf.

261 DHS also regularly takes advantage of other Privacy Act exemptions, one of which is the "routine use" exemption that allows agencies to share records without the consent of the individual to whom the record pertains "for a purpose which is compatible with the purpose for which [the record] was collected." 5 U.S.C. § 552a(a)(7) (2014). See Saira Hussain and Sophia Cope, "Deep Dive: CBP's Social Media Surveillance Poses Risks to Free Speech and Privacy Rights," Electronic Frontier Foundation, August 5, 2019, https://www.eff.org/deeplinks/2019/08/deep-dive-cbps-social-media-surveillance-poses-risks-free-speech-and-privacy. Although this exemption has been interpreted narrowly by courts, DHS frequently invokes it in SORNs to justify granting itself increasingly vast authority to disclose individuals' personal information in ways inconsistent with the Privacy Act. U.S. Postal Serv. v. Nat. Ass'n, Letter Carriers, 9 F. 3d 138 (D.C. Cir. 1993); EPIC, "Comments of the Electronic Privacy Information Center to the Department of Homeland Security," docket nos. DHS-2020-0015 and DHS-2020-0014, January 13, 2020, https://epic.org/wp-content/uploads/apa/comments/EPIC-Comments-DHS-

Counterintelligence-SORN-January-2021.pdf; and EPIC, "Comments of the Electronic Privacy Information Center to the Department of Homeland Security," docket nos. DHS-2017-0001 and DHS-2020-0002, June 5, 2017, 9, https://epic.org/wp-content/uploads/apa/comments/EPIC-DHS-FALCON-Database-Comments.pdf.

262 OIG, *DHS Privacy Office Needs to Improve Oversight*, 6. PIAs are preceded by privacy threshold analyses, which must be completed by the component for the privacy office's review. OIG, *DHS Privacy Office Needs to Improve Oversight*, 5.

263 See Privacy Office, "DHS-CBP-PIA-007 Electronic System for Travel Authorization," DHS, accessed December 21, 2021, https://www.dhs.gov/publication/electronic-system-travel-authorization; Privacy Office, "DHS/CBP/PIA-006 Automated Targeting System," DHS, accessed December 21, 2021, https://www.dhs.gov/publication/automated-targeting-system-ats-update; and Privacy Office, "DHS/CBP/PIA-021 TECS System: Platform," DHS, accessed December 23, 2021, https://www.dhs.gov/publication/dhscbppia-021-tecs-system-platform.

264 Philip S. Kaplan, *Privacy Impact Assessment for the Traveler Verification Service*, DHS Privacy Office, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

265 42 U.S.C. § 2000ee–3 (2007) (subject-based data analysis or searches that start with personal identifiers do not count as data mining, nor do searches for historical trends).

266 6 U.S.C. § 142. Details about how these reviews are carried out are found in various Privacy Office publications. See, e.g., DHS, "Instruction Number 047-01-004: Chief Privacy Officer, Privacy Compliance Reviews," January 19, 2017, https://www.dhs.gov/sites/default/files/publications/Instruction%20047-01-004%20Chief%20Privacy%20Officer%20Privacy%20Compliance%20Reviews.pdf.

267 Privacy Office, "Privacy Compliance Review Standard Operating Procedure," DHS, November 2016, 1, https://www.dhs.gov/sites/default/files/publications/PCR%20SOPs%20FINAL_0.pdf.

268 Privacy Office, "Privacy Compliance Review (PCR) Open Recommendations," DHS, January 8, 2021, https://www.dhs.gov/sites/default/files/publications/pcr_open_recommendations_november_2020.pdf.

269 In 2012, then–Chief Privacy Officer Jonathan Cantor testified before Congress about privacy concerns with body scanners. He explained that the Privacy Office works closely with DHS components in the course of rolling out new technologies to develop "privacy-mitigation strategies," but it does not appear that the Privacy Office would advise a component *not* to use a particular technology, except perhaps in rare circumstances. *TSA's Recent Scanner Shuffle: Real Strategy or Wasteful Smokescreen*, *Hearing Before the Subcomm. on Transportation Security of the H. Comm. on Homeland Security*, 112th Cong. (2012) (testimony of Jonathan Cantor, acting chief privacy officer, DHS) https://www.govinfo.gov/content/pkg/CHRG-112hhrg81130/html/CHRG-112hhrg81130.htm.

270 EPIC, "Department of Homeland Security Chief Privacy Office and Privacy," accessed December 17, 2021, https://epic.org/privacy/dhs-cpo.html.

271 Inspector General Act of 1978, 5a U.S.C.C.A. 95-452, § 3.

272 Inspector General Act of 1978, 5a U.S.C.C.A. 95-452, § 5. Although national security agencies can invoke an exceptional power to interfere with IG investigations or reports, they have almost never used this power.

273 U.S. Customs and Border Protection Authorization Act, 6 U.S.C. § 211(k)(5) (2020).

274 OIG's early practice was to publish a report summarizing its significant investigations for the preceding period. Since 2013, OIG has instead incorporated less detailed summaries of some significant investigations into its semiannual reports to Congress. See, e.g., OIG, *Semiannual Report to the Congress, October 1, 2020–March 31, 2021*, June 1, 2021, https://www.oig.dhs.gov/sites/default/files/assets/SAR/2021/oig-sar-oct20-mar21.pdf.

275 Government Accountability Project to Rep. Elijah Cummings et al., June 27 2019, https://www.whistleblower.org/wp-content/uploads/2019/06/Congressional-Letter-OIG-CRCL-Failures.pdf.

276 OIG, *TSA Needs to Improve Management of the Quiet Skies Program*.

277 As has been extensively reported, OIG has been beset by severe internal management issues that have substantially undermined its reputation and culture. See Geneva Sands and Zachary Cohen, "Watchdog Investigating DHS Inspector General Over Retaliation Claims," CNN, https://www.cnn.com/2022/02/11/politics/dhs-inspector-general-investigated-watchdog-group/index.html; Ken Klippenstein, "Inside the Brutal Power Struggle at Homeland Security," *Intercept*, February 2, 2021, https://theintercept.com/2021/02/02/homeland-security-power-struggle-cuffari; John Hudak and Grace Wallack, "Political Appointees as Barriers to Government Efficiency and Effectiveness: A Case Study of Inspectors General," Brookings Institution, April 2016, https://www.brookings.edu/wp-content/uploads/2016/07/oig.pdf; and Sens. Claire McCaskill and Ron Johnson, "Investigation into Allegations of Misconduct by the Former Acting and Deputy Inspector General of the Department of Homeland Security," staff report, Subcomm. on Financial and Contracting Oversight of the S. Comm. on Homeland Security and Governmental Affairs, April 24, 2014, https://s3.documentcloud.org/documents/1146994/edwards-senate-investigation.pdf.

278 Cordero, *Reforming the DHS*.

279 DHS, "Homeland Security Advisory Council," accessed March 17, 2022, https://www.dhs.gov/homeland-security-advisory-council.

280 One avenue would be for the chief privacy officer, in coordination with the secretary of homeland security, to reinvigorate DHS's Data Privacy and Integrity Advisory Committee (DPIAC) to assist the office in addressing foundational questions about programs — for example, by drawing on the comprehensive risk assessment process it designed in 2006 — rather than simply responding to narrow questions posed by department leadership. DPIAC, *Framework for Privacy Analysis of Programs, Technologies, and Applications*, DHS, March 7, 2006, https://www.dhs.gov/sites/default/files/publications/DPIAC%20Recommendations%20Paper%202006-01.pdf.

281 Congress should also consider conferring subpoena power upon CRCL to enhance its ability to obtain information from DHS components.

ABOUT THE AUTHORS

▶ **Faiza Patel** is a nationally recognized expert on counterterrorism and government surveillance. As codirector of the Brennan Center's Liberty and National Security Program, she has published research on NSA surveillance, social media monitoring, countering violent extremism, and targeting of Muslim communities. Patel has testified before the Senate and House of Representatives on homeland security surveillance. Her writing has been featured in major publications such as the *New York Times*, the *Washington Post*, and the *Los Angeles Times.* She is also a regular contributor to the legal blog *Just Security*, for which she is a member of the board of editors. Previously, she worked as a senior policy officer at the Organization for the Prohibition of Chemical Weapons in The Hague and served as a law clerk at the International Criminal Tribunal for the former Yugoslavia.

▶ **Rachel Levinson-Waldman** is deputy 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 the government's use of social media, Fourth Amendment implications of public space surveillance, and the federal government's retention and sharing of noncriminal information about Americans. She has written and provided expert input for publications including the *Guardian*, the *Washington Post*, *Wired*, the *Atlantic*, and the *New Republic*. She previously served as senior counsel to the American Association of University Professors and trial counsel in the Civil Rights Division of the U.S. Department of Justice, and as a law clerk to the Honorable M. Margaret McKeown of the U.S. Court of Appeals for the Ninth Circuit.

▶ **Harsha Panduranga** is counsel in the Brennan Center's Liberty and National Security Program. He advocates for public safety policies that serve those they are meant to protect and are rooted in proof, not prejudice. He has authored or coauthored four Brennan Center reports: *Community Investment, Not Criminalization* (2021), *Government Access to Mobile Phone Data for Contact Tracing* (2020), *Extreme Vetting and the Muslim Ban* (2017), and *Trump-Russia Investigations: A Guide* (2017). Panduranga has served as legal counsel in cases challenging the Muslim ban and the federal government's dragnet monitoring of social media. His work and commentary have been featured in media outlets including the *Atlantic*, *Slate*, *Politico*, NPR, *BuzzFeed*, the *Daily Beast*, *Lawfare*, and *Just Security*. Prior to joining the Brennan Center, Panduranga was a litigation associate at Simpson Thacher & Bartlett LLP. He received his BA and JD from the University of Michigan.

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 the Bauman Foundation, 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 would like to express their gratitude to the Brennan Center's Lisa Benenson, Julian Brookes, Matthew Harwood, Zachary Laub, Alexandra Ringe, Janet Romero-Bahari, and Alden Wallace for their editing and communications assistance. We are also grateful to Mary Pat Dwyer, Mike German, Liza Goitein, and Laura Hecht-Felella for their research and drafting contributions and their expert input, and to José Gutiérrez, Priyam Madhukar, Kaylana Mueller-Hsia, Alia Shahzad, and Sahil Singhvi for their tireless research and cite checking, as well as undergraduate and legal interns Sarah Guinee, Sean Lau, Bianny Magarin, and Jesús Rodríguez. We appreciate the guidance and support of Michael Waldman and John Kowal. Finally, we are deeply grateful to the many outside experts who generously shared their time and subject matter expertise, including Joan Friedland, Jim Harper, Edward Hasbrouck, Liz Hempowicz, Chappell Lawson, Greg Nojeim, Harrison Rudolph, Jeramie Scott, Scott Shuchart, and Jana Winter, as well as current and former DHS officials and others who wish to remain anonymous.

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