BRENNAN CENTER FOR JUSTICE

A Course Correction for Homeland Security

PUBLISHED APRIL 20, 2022

According to its founding statute, the Department of Homeland Security (DHS) is primarily charged with protecting the country against terrorist attacks. But the agency's post-9/11 strategies have too often targeted vulnerable communities with scant evidence of effectiveness. With DHS's 20th anniversary around the corner, it is time to take a step back. While the breadth of management and mission 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.

One area in dire need of a closer look is DHS's execution of its counterterrorism authorities. A new Brennan Center report finds that a toxic combination of broad authorities, weak safeguards, and inadequate oversight have allowed problems with DHS's counterterrorism mandate to fester for 20 years.

DHS's counterterrorism partnerships with state and local law enforcement and private actors are plagued by inadequate controls and have too often been used to target minorities and protest movements.

- DHS's central intelligence unit, the Office of Intelligence and Analysis (I&A), has weak rules and safeguards. As a result, political priorities have often driven intelligence priorities. Most recently, the office has monitored protestors in Portland, issued intelligence bulletins on journalists, and elevated the threat from racial justice protests while downplaying the threat from white supremacists in the run-up to the January 6, 2021, attack on the Capitol.

- I&A provides support and guidance to fusion centers, state-run intelligence-sharing hubs that have repeatedly disseminated unreliable information and surveilled Black Lives Matter activists and other protestors.

- The department's violence prevention program, which administration officials concede was unfairly targeted at American Muslims, has been rebranded twice and supposedly broadened to cover all types of "targeted violence." But overt bias is not the only problem with these efforts: not only have they never been shown to actually prevent violence, but their vague and broad criteria open the door to profiling.

DHS uses its counterterrorism and screening mandates to accumulate massive amounts of data on Americans with minimal transparency and few checks to prevent abuse.

- DHS draws from a wide range of sources — including biometrics, purchases of location data, social media

posts, and information from warrantless border searches of laptops and phones — and shares that data widely among its different operations.

- There is no comprehensive accounting of what happens with all that data, making it impossible for the public to know what is collected or how it is used.

- DHS uses this personal information to make opaque determinations about individual travelers' risk levels, singling out some for questioning, detention, and even harassment or bars on travel.

- Outside observers and DHS officers themselves have accused border agents of subjecting Muslim, Black, and Hispanic travelers to heightened scrutiny at airports.

- According to former senior DHS officials, the privacy and due process concerns posed by the department's accumulation of information about Americans dwarf those arising from the National Security Agency's data collection.

DHS's oversight infrastructure, which comprises primarily the Privacy Office, the Office for Civil Rights and Civil Liberties (CRCL), and the Office of Inspector General (OIG), has frequently been unable — and in some cases unwilling — to prevent or rein in abuses in counterterrorism programs.

- Congress wisely established these internal oversight entities in recognition of the risks posed by DHS's vast array of programs. But these offices have had limited influence and authority, to the detriment of both the department and the broader public.

- While the Privacy Office and CRCL are required to produce public reports, these documents often either provide minimal information or discuss counterterrorism and screening programs and technologies in vague and opaque language.

- OIG has repeatedly concluded that DHS has failed to ensure the efficacy of new counterterrorism programs before rolling them out and also failed to establish ways to measure their effectiveness once implemented.

- All three oversight entities tend to focus on procedural fixes and frequently avoid substantive concerns.

Recommendations

A course correction is critical. We urge the secretary of homeland security to take the following steps:

- **Strengthen safeguards against profiling.** DHS should close loopholes in its policies on nondiscrimination to explicitly cover religion and national origin, and to more stringently limit the use of protected characteristics such as race, religion, and ethnicity. Fusion centers and other DHS-funded entities should adopt similar policies.

- **Protect privacy and free expression.** As recommended by its Office of the General Counsel, DHS should conduct a wholesale review of the Office of Intelligence and Analysis. It should also reinstitute CRCL oversight of I&A's intelligence products (a practice scrapped under the Trump administration) and develop a formal policy to protect individuals' and groups' First Amendment rights. Reasonable suspicion of criminal activity or criminal planning should be the basis for creating, maintaining, or sharing records of Americans' personal information.

- **Evaluate the efficacy of counterterrorism and screening programs.** The department's failure to measure or establish the efficacy of its programs has resulted in overreach, aggressive data grabs, and violations of individuals' civil rights and civil liberties. DHS should institute a rigorous process to ensure that its initiatives actually fulfill their stated goals.

- **Ensure meaningful transparency.** DHS should map out and publish a holistic review of how it takes in, uses, and retains Americans' personal data. DHS leadership should empower the Privacy Office and CRCL to provide more detailed, comprehensive, and useful information in their public reports.

- **Foster robust oversight.** DHS leadership should publicly support and internally empower the Privacy Office and CRCL. The Privacy Office should be asked to weigh in on *whether* the department should undertake certain initiatives or adopt certain technologies, not just *how* to implement them, and CRCL should be given structural opportunities to provide input and oversight. Additionally, DHS should establish accountability mechanisms for components that fail to provide information and support to internal oversight offices.

These reforms would help rein in abuses in DHS counterterrorism programs and improve oversight and effectiveness, allowing the department to better protect all Americans. The secretary can — and should — make these changes now.