Re: Docket No. PCLOB-2022-0001

To the members of the Privacy and Civil Liberties Oversight Board:

We are pleased to provide this response to the PCLOB’s request for comments on the agenda for the upcoming public forum on privacy and liberties issues concerning the government’s efforts to counter domestic terrorism. While we recognize the need to combat far-right violence more effectively, we are concerned that many of these efforts will erode core constitutional protections and work to the detriment of the very communities that are most affected by it. We ask, in particular, that the agenda include significant attention to the impacts of these efforts on First Amendment-protected activities and on racial, religious, and other minority groups, with specific attention to the topics discussed below. These impacts are often attributable to a framework that emphasizes ideology over action and affords broad discretion to law enforcement to conduct investigations and surveillance without requiring individualized suspicion of violent criminal activity. We then examine the intersection of these two areas of concern with the use of technology, namely social media tracking.

We also include here four Brennan Center reports touching on the topics discussed below that may be useful to the Board as it undertakes its work: 1) A Course Correction for Homeland Security: Curbing Counterterrorism Abuses; 2) Community Investment, Not Criminalization; 3) Social Media Monitoring; and 4) National Security and Local Police. Please let us know if we can provide additional recommendations regarding resources or speakers who can speak to these impacts as the Board constructs its agenda for the forthcoming public forum.

1. Framework to address domestic terrorism captures ideology and other non-criminal activity

Our first area of concern is that federal law enforcement defines its mandate to address domestic terrorism too broadly, capturing activity protected by the First Amendment and opening the door to the targeting of minority communities.

a. Going beyond the statutory definition of domestic terrorism

Federal law defines domestic terrorism (DT) roughly as criminal acts dangerous to human life occurring within the United States that appear intended to target the public or influence government policy through intimidation or coercion. Departing from this statutory definition, counterterrorism agencies also use the supplementary “domestic violent extremism” (DVE) framework as part of their DT efforts, even though this term is not consistently defined across the government, creating confusion about precisely what activity is covered. The DVE framework opens the door for law

---


2 18 U.S. Code § 2331(5).

3 As a recent Department of Homeland Security (hereinafter DHS) document noted in recommending the adoption of a consistent definition of DVE: “Multiple definitions of domestic violent extremism and violent extremist activity are
enforcement to selectively target individuals based on activity protected by the First Amendment—that is, based on whether they are perceived to have “extremist” views rather than whether they have engaged in, or credibly threatened to engage in, violence that fits the legal definition of terrorism.

The Federal Bureau of Investigation’s (FBI) DVE framework—which the Department of Homeland Security (DHS) and the Intelligence Community have adopted—is organized around ideologies rather than a record of violence or operational links. It groups the documented threat of violent white supremacy with the largely unsubstantiated threat of Black separatism under the umbrella of Racially or Ethnically Motivated Violent Extremists, and includes within the Abortion-Related Violent Extremists classification a category of pro-choice DVEs, although there is no evidence that such a movement exists. As a result, in addition to centering ideology in place of suspicion of violent criminal activity, the DVE framework obscures serious threats of violence and elevates less serious or non-existent ones. Further, combining within a single category groups that do not work with each other—and in fact often stand in opposition—makes little sense if the goal of such a grouping is more efficiently pooling intelligence and law enforcement resources.

b. “Violence prevention” as law enforcement overreach

The same basic notion that factors untethered to suspicion of violent criminal activity are an appropriate focus of counterterrorism efforts plagues DHS’s violence prevention initiatives, coordinated by its Center for Prevention Programs and Partnerships (CP3), which was rolled out in May 2021. CP3 grows out of the countering violent extremism (CVE) programs of the Obama era, which relied on widely discredited theories of terrorist radicalization that painted Muslim religious practices and the expression of political grievances as precursors to terrorist violence. Although these programs have run for years, DHS’s evaluations of them have failed to measure whether they actually reduce violence, instead relying on proxies such as the number of trainings or the establishment of mechanisms for reporting.

DHS officials have conceded that CVE was biased due to its focus on “specific religious and ethnic communities,” but the department has not grappled with the flaws in the underlying policy
framework.\(^\text{10}\) Instead, through CP3, it has expanded the model with the goal of addressing a broader range of violence than only terrorism associated with Muslims, with “domestic violent extremism” as a point of stated emphasis.\(^\text{11}\) Like CVE, CP3 also seeks—directly and through grants—to train law enforcement officials, educators, public health officials, social workers, and private citizens to identify and report people who show purported warning signs that they might commit an act of “targeted violence” or terrorism sometime in the future.\(^\text{12}\) These supposed indicators include some combination of vague and commonplace characteristics like holding a grievance, having an “extremist” view, being socially isolated, and feeling hopeless.\(^\text{13}\)

All of these signs are so overbroad as to be meaningless and allow for well-documented biases to inform who is perceived as dangerous.\(^\text{14}\) Indeed, directing law enforcement agents and their proxies to counter “radical” ideologies or identify ill-defined “concerning behaviors” will undoubtedly lead to the targeting of marginalized groups exercising their constitutionally protected rights to challenge the status quo, rather than white supremacists who have long been deeply embedded in powerful government institutions like law enforcement and the military. History provides ample evidence of this point: law enforcement has long treated as “radical” ideas that have stood in opposition to established structures of power, such as civil rights, labor organizing, or women’s suffrage.\(^\text{15}\)

### 2. Dearth of safeguards for domestic intelligence collection

Since 9/11, intelligence collection and sharing programs have grown exponentially. While it is important to ensure that law enforcement agencies collect and share credible information about

---


\(^\text{11}\) DHS, “Center for Prevention Programs and Partnerships,” (under “CP3 Background”).

\(^\text{12}\) See generally Panduranga, Community Investment, Not Criminalization.


actual threats of violence, the weakening of safeguards over the last two decades—combined with new and powerful tools for collecting information—have resulted in the collection and dissemination of false, biased, and unreliable information, with little accountability, often untethered from criminal activity, and focused on constitutionally protected speech. As the administration concentrates on domestic terrorism, the risks for Americans are magnified.

a. FBI

For the last two decades, the FBI has exercised increasingly broad authority to collect information about Americans not suspected of criminal activity. For example, the 2008 Attorney General’s Guidelines for Domestic FBI Operations (AG Guidelines), issued by Attorney General Michael Mukasey, permit agents to open “assessments” based on a broadly defined “authorized purpose,” such as preventing crime or terrorism.16 During an assessment, agents may recruit and task informants, map communities on the basis of race and ethnicity, and conduct physical surveillance, database searches, and interviews.17 The jettisoning of one of the key reforms triggered by the 1975 investigation carried out by the Church Committee—the requirement of a factual predicate for investigations—has given the FBI immense discretion in selecting targets and has opened the door to targeting people on the basis of ideology, unwarranted intrusions of privacy, and racial, religious, and ethnic profiling.18

The AG Guidelines do bar investigations and surveillance “solely for the purpose of monitoring activities protected by the First Amendment.”19 But this has not served as an effective safeguard: it is easy to cite a pretextual but constitutionally neutral justification (for example, an unsubstantiated contention that a protest could turn violent) to collect information on Americans’ political organizing and religious practices. Likewise, the 2014 Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity has done little to constrain these authorities—among other loopholes, it exempts “threats to national or homeland security,” permitting agents to consider protected traits without individualized suspicion of wrongdoing.20

Indeed, the FBI has marked minority communities, activists, and protest movements for investigation. In the post 9/11 era, the FBI has routinely targeted Muslims absent suspicion of any criminal activity, infiltrating mosques and manufacturing terrorism prosecutions of young Muslim

---

19 AG Guidelines, 13.
men using sting operations.\textsuperscript{21} A leaked 2017 FBI intelligence assessment also described the creation of a new domestic terrorism category called “Black Identity Extremism,” based on the claim that some Black activists opposing police brutality may pose a violent threat to law enforcement.\textsuperscript{22} The term was used to justify a nationwide operation called “Iron Fist,” in which FBI agents engaged in enhanced surveillance and investigations of Black activists.\textsuperscript{23}

The Justice Department also exploited the FBI’s pervasive authorities to launch the “China Initiative.” The China Initiative targeted Chinese and Chinese-American scientists and technologists for investigation and selective prosecution based on their race and national origin (often referred to as a “nexus” to China), and encouraged academic institutions to closely monitor Asian students and faculty in a misguided effort to combat economic espionage.\textsuperscript{24} The China Initiative was, commendably, ended in February 2022, with the Justice Department acknowledging that it “helped give rise to a harmful perception…that we in some way view people with racial, ethnic or familial ties to China differently.”\textsuperscript{25} The department will continue investigating economic espionage without a program focused on one country, but questions remain, including regarding how it will proceed with pending cases brought under the prior framework.\textsuperscript{26}

b. DHS Office of Intelligence and Analysis (I&A)

DHS’s Office of Intelligence and Analysis (I&A) operates under permissive authorities as well. I&A undertakes surveillance in support of counterterrorism and other “authorized intelligence


\textsuperscript{26} Michael German and Alex Liang, “End of Justice Department’s ‘China Initiative’ Brings Little Relief to U.S. Academics,” Brennan Center for Justice, March 25, 2022, \url{https://www.brennancenter.org/our-work/analysis-opinion/end-justice-departments-china-initiative-brings-little-relief-us}.
missions,” relying primarily upon open-source information. This information is shared broadly with federal, state, local, tribal, and territorial agencies, shaping their perception of and response to activities within their jurisdictions. The office is not allowed to undertake intelligence activities “for the sole purpose of monitoring” constitutionally or legally protected activities, but this weak safeguard has failed in preventing overreach and abuses by I&A agents and officials.

Throughout I&A’s history, the office’s reports have periodically drawn criticism for targeting groups on the basis of protected characteristics or First Amendment-protected activity. A notable recent example is I&A’s dissemination of intelligence reports on journalists covering its monitoring of racial justice protestors in the summer of 2020. I&A conducted this surveillance of constitutionally-protected activity under the theory that the potential vandalism of monuments, memorials and statues posed a “significant threat to homeland security,” raising alarms regarding overreach in Congress and among the public. A March 2022 report by DHS’s Inspector General noted that I&A published 366 reports in reaction to those protests, and also that it did not publish any reports between the November 2021 presidential election and the January 6 Capitol attack, a fact that raises serious questions about the office’s objectivity.

I&A works closely on efforts to counter domestic terrorism with fusion centers, which are hubs for sharing information between state, local and federal authorities. A decade ago, a 2012 bipartisan Senate investigation reported that fusion centers “yielded little, if any, benefit to federal counterterrorism intelligence efforts,” instead producing reams of low-quality information and putting scrutiny on Muslim groups engaging in innocuous activities such as hosting events on subjects like marriage and “positive parenting.” Reports of similar problems have persisted in the decade since then. For example, fusion centers have been caught monitoring racial justice and Muslim activism, Juneteenth celebrations, environmental advocates, and people demonstrating on issues ranging from women’s rights to the government response to Hurricane Maria in Puerto Rico.

28 I&A, Intelligence Oversight Program and Guidelines, 2.
The federally established information-sharing mechanisms used by these centers also do not follow 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. Further, I&A’s audits of these centers rely almost exclusively on self-reporting; it does not undertake any substantive review of the intelligence that fusion centers distribute, in contrast to the 2012 Senate investigation that unearthed systemic problems with fusion centers’ functioning.

3. Social media tracking

Social media tracking has become a go-to tool for security agencies, including in their efforts to combat domestic terrorism. According to the 2021 National Strategy for Countering Domestic Terrorism, the federal government intends to draw on “open-source information”—some of which will be derived from social media—to identify potential domestic terrorism threats. While specific investigations supported by a factually-predicated suspicion of criminal activity may require law enforcement agencies to review social media, the broadscale monitoring of social media with the goal of identifying potential threats of violence or terrorism raises serious First Amendment and privacy concerns, and will have a disproportionate impact on communities that have historically borne the brunt of law enforcement overreach. In addition, there is little proof that it will work. Nevertheless, both the FBI and DHS have reportedly hired private firms and sought to leverage automated tools to help conduct such surveillance.


When a government agency collects social media information, it has the ability to create detailed dossiers of Americans’ views, including political matters that lie at the heart of First Amendment protections, as well as their social networks and even where they are located and the places they go. Indeed, a person’s social media presence—their posts, comments, photos, likes, group memberships, and so on—can collectively reveal their ethnicity, political views, religious practices, gender identity, sexual orientation, personality traits, and vices. Thus, as the FBI’s investigations guide recognizes, “[o]nline information, even if publicly available, may still be protected by the First Amendment.”

Further, social media can reveal more about a person than they intend. Platforms’ privacy settings change frequently and can be difficult to navigate, and even when individuals keep information private it can be disclosed through the activity or identity of their connections on social media. DHS has recognized this risk, categorizing social media handles as “sensitive personally identifiable information” that “could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual” if disclosed without consent.

People are likely to censor themselves if they think they are being watched by the government, including on social media, which can make them reluctant to speak about controversial or personal issues. This undermines everything from political speech to creative output to other forms of self-expression. Social media monitoring can also blur the line between scrutiny of constitutionally protected activity and examination of genuine threats of violence. There are myriad examples, for example, of proposals to abuse social media for the purposes of political repression, with the FBI in particular accused of misusing social media data.

41 See Elizabeth Stoycheff et al., “Privacy and the Panopticon: Online Mass Surveillance’s Deterrence and Chilling Effects,” New Media & Society 21 (2018); Dawinder S. Sidhu, “The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim Americans,” University of Maryland Law Journal of Race, Religion, Gender & Class 7 (2007); and Elizabeth Stoycheff, “Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring,” Journalism & Mass Communication Quarterly 93 (2016): 307-308. A recent lawsuit by the Brennan Center and the Knight First Amendment Institute against the State Department and DHS documents how the collection of social media identifiers on visa forms led a number of international filmmakers to stop talking about politics and promoting their work on social media because they were concerned that what they said online would prevent them from getting a U.S. visa or be used to retaliate against them. Complaint, Doc Society v. Pompeo, No. 1:19-cv-03632-TJK (D.D.C. December 5, 2019).
instance, of the FBI and DHS using social media to monitor people speaking out on issues from racial justice to the treatment of immigrants.42

Nor is tracking what people say on social media likely to help identify national security threats with any reliability. DHS’s internal assessments of its pilot programs using social media to screen certain applicants for immigration benefits found them practically useless, with officers having difficulty using social media to pinpoint fraud or national security concerns.43 Further, as DHS has repeatedly acknowledged, it is difficult to locate and interpret true threats of violence on social media—unsurprisingly, as social media is highly context-specific and can be riddled with slang, jokes, memes, sarcasm, and references to popular culture.44 Automated tools that claim to make judgments about which threats, calls for violence, or individuals actually pose a genuine threat of violence are also prone to error. As more than 50 technologists wrote in opposing an ICE proposal aimed at predicting whether a given person would commit a crime or terrorist act, these tools are simply not capable of making such determinations, both because such judgments are subjective and they are trying to predict statistically rare events.45 Similar concerns apply to mechanisms used to flag images and videos, which generally lack the context necessary to distinguish a scenario in which an image is used for reporting or commentary from one where it is used with the intention of inciting violence.46

Conclusion

We appreciate the opportunity to provide these comments and look forward to offering additional input and information as the PCLOB undertakes the important effort of addressing the privacy and liberties issues raised by the government’s efforts to counter domestic terrorism. Please do not hesitate to let us know if we can provide any further information. We may be reached at patelif@brennan.law.nyu.edu (Faiza Patel), levinsonr@brennan.law.nyu.edu (Rachel Levinson-Waldman), and pandurangah@brennan.law.nyu.edu (Harsha Panduranga).

Respectfully submitted,

Brennan Center for Justice