June 30, 2022

Privacy and Civil Liberties Oversight Board
2100 K Street NW, Suite 500
Washington, DC 20427

Dear Privacy and Civil Liberties Oversight Board Members:

On behalf of the American Civil Liberties Union (ACLU), a non-partisan organization with over two million members, activists, and supporters nationwide, we are pleased to provide comments regarding the Privacy and Civil Liberties Oversight Board's (PCLOB) public forum on "privacy and civil liberties in the domestic terrorism context."[1]

In light of recent mass shootings and the surge in white supremacist violence, both the executive and legislative branches have renewed efforts to address "domestic terrorism" in the United States. Indeed, last year, President Biden announced the first-ever national strategy to counter domestic terrorism, rightly emphasizing America's history and present escalation of white supremacist violence and the chronic contributors to that violence, including racism and bigotry.[2] We appreciate that the strategy also stressed that responses to domestic threats must ensure the protection of cherished civil rights and civil liberties. But we have serious concerns about the impact of government efforts on civil rights and liberties, and much work must be done to ensure that these efforts comport with our nation's obligations to all of its people.

The ACLU welcomes the PCLOB's interest in evaluating the impacts that these efforts have on individual rights, especially for communities of color, immigrants, and other marginalized communities. History has shown that even well-intentioned government measures to address security concerns—including the increased use of both traditional and novel surveillance technologies—can harm the very communities that are often the focus of white supremacist violence.

The starting point for the PCLOB's focus should be that current domestic national security and counterterrorism policy is deeply flawed. That policy reflects the government's ever-expanding authority[3] to surveil and monitor American communities; [4] law enforcement

[1] U.S. Privacy and C.L. Oversight Bd., Notice of Public Forum, 87 Fed. Reg. 19536-37 (Apr. 4, 2022).

[2] *See* White House, FACT SHEET: National Strategy for Countering Domestic Terrorism (June 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/fact-sheet-national-strategy-for-countering-domestic-terrorism.

[3] Liliana Segura, *Gutting Habeas Corpus: Inside Story of How Bill Clinton Sacrificed Prisoners' Rights for Political Gain*, Intercept (May 4, 2016), https://theintercept.com/2016/05/04/the-untold-story-of-bill-clintons-other-crime-bill.

[4] *Surveillance Under the USA/Patriot Act*, ACLU, https://www.aclu.org/other/surveillance-under-usapatriot-act (last visited June 29, 2022).

guidance that permits profiling on the basis of race, religion, national origin, and other protected characteristics; [5] and the use of abusive tools such as the watchlisting system against people exercising constitutionally protected speech and association.[6] For the past 20 years—and longer—these approaches have disproportionately targeted Black, Brown, Muslim, and immigrant communities through the lens of "security threat,"[7] and have harmed the rights to free expression, due process, and equal protection under the law.[8]

Moreover, law enforcement already enjoys a vast array of authorities, from investigation through prosecution, that allow it to address white supremacist violence effectively. Congress has passed more than 50 statutes that relate to domestic terrorism offenses and material support for terrorism.[9] Should the PCLOB receive proposals recommending new crimes or law enforcement authorities, it should view them with hesitation, if not skepticism. What's more, the authorities that law enforcement agencies already possess have been used by the federal government to wrongly target vulnerable populations—Black civil rights activists, Muslim, Arab, Middle Eastern, and South Asian communities, animal rights and environmental rights activists, and other groups the government views as having "unpopular" or controversial beliefs.

During the civil rights movement, leaders like Martin Luther King, Jr. were investigated and monitored based upon their organizing and civil disobedience in the pursuit of equal rights. More recently, the FBI has used the USA Patriot Act's definition of "domestic terrorism" to investigate and surveil individuals—including those engaged in First Amendment–protected activities—with little basis.[10] The agency has used domestic

---

[5] U.S. Dep't of Justice, Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (Dec. 2014), https://www.dhs.gov/sites/default/files/publications/use-of-race-policy_0.pdf.

[6] Hugh Handeyside, *The Watchlisting System Exemplifies the Government's Post-9/11 Embrace of Biased Profiling*, ACLU (Sept. 9, 2021), https://www.aclu.org/news/national-security/the-watchlisting-system-exemplifies-the-governments-post-9-11-embrace-of-biased-profiling.

[7] Human Rights Watch, Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions (July 2014), https://www.hrw.org/report/2014/07/21/illusion-justice/human-rights-abuses-us-terrorism-prosecutions.

[8] *Top Ten Abuses of Power Since 9/11*, ACLU, https://www.aclu.org/other/top-ten-abuses-power-911 (last visited June 29, 2022).

[9] Roy L. Austin Jr. & Kristen Clarke, *Creating a 'domestic terrorism' charge would actually hurt communities of color*, Wash. Post (Aug. 26, 2019), https://www.washingtonpost.com/opinions/domestic-terrorism-doesnt-need-to-be-a-chargeable-offense-we-already-have-powerful-hate-crime-laws/2019/08/26/14c6f354-c4eb-11e9-b72f-b31dfaa77212_story.html.

[10] Press Release, ACLU, New Documents Show FBI Targeting Environmental and Animal Rights Groups Activities as "Domestic Terrorism" (Dec. 20, 2005), https://www.aclu.org/news/new-documents-show-fbi-targeting-environmental-and-animal-rights-groups-activities-domestic.

terrorism authorities to spy upon Muslim communities, including by infiltrating their places of worship.[11]

This must change, and this Board should do its part to ensure that it does. Federal government agencies must implement meaningful civil rights, liberties, and privacy safeguards to protect communities of color, immigrant, and other vulnerable communities from law enforcement abuses of national security-based authorities—and the deeply consequential harms to people's personal and professional lives that result.

The ACLU recommends that the PCLOB begin to address these issues by taking the following three steps: (1) examine the impact of the Department of Justice Guidance on Race and Federal Bureau of Investigation's Domestic Investigations and Operations Guide on the discriminatory profiling of communities of color, immigrants, and other vulnerable communities; (2) make public key information about the Center for Prevention, Programs, and Partnerships and assess the program's impact on civil rights and civil liberties; and (3) comprehensively map and make public the many surveillance and information-processing systems DHS uses for counterterrorism purposes, including systems that DHS is deploying or expanding to track and predict "domestic violent extremism."

I. Department of Justice and Department of Homeland Security Investigations and Guidance on Racial Profiling

Federal law enforcement agencies' use of domestic terrorism authorities flows in part from the USA Patriot Act of 2001, which enacted—for the first time—a definition of "domestic terrorism." That definition is vague, overbroad, and malleable. It covers criminal acts "dangerous to life" that "appear to be intended to" intimidate or coerce the public or the government.[12] Federal agencies have used this definition to claim expansive investigative authorities that have harmed communities of color, immigrants, and other marginalized communities, including those engaged in First Amendment–protected activities. Although both the Department of Justice and the Department of Homeland Security have issued guidance that purports to prohibit biased profiling, both include glaring loopholes that allow law enforcement and intelligence gathering agencies to target vulnerable communities under the guise of national and border security.

After Congress enacted the USA Patriot Act "domestic terrorism" definition, the Department of Justice (DOJ) loosened safeguards in its Attorney General investigative guidelines for Federal Bureau of Investigation (FBI) operations, and the FBI's Domestic

[11] Janet Reitman, *I Helped Destroy People*, N.Y. Times (Sept. 1, 2021), https://www.nytimes.com/2021/09/01/magazine/fbi-terrorism-terry-albury.html.

[12] USA Patriot Act, Pub. L. No. 107–56, § 802, 115 Stat. 376 (2001) (codified as amended at 18 U.S.C. § 2331).

Investigations and Operations Guide (DIOG), issued pursuant to those guidelines.[13] Under the Attorney General guidelines and the DIOG, agents can open "assessments" without any factual basis for suspicion of actual criminal wrongdoing.[14] During these investigations, agents are permitted to use invasive techniques for data-gathering, such as racial and ethnic mapping, confidential informants, physical surveillance, and commercial and law enforcement database searches.[15] Under these rules, the FBI has also analyzed the location of ethnic-oriented businesses and facilities based on crude stereotypes about specific minority communities' propensity to crime.[16] Federal intelligence and law enforcement agencies use these authorities to unfairly target people of color and other marginalized communities for surveillance, investigation, prosecution, and placement on watchlists.[17] The FBI has also used domestic terrorism authorities to spy on Muslim communities, including by infiltrating their places of worship.[18] In 2010, the DOJ Inspector General criticized the FBI for misusing its authority by treating potential crimes, such as non-violent civil disobedience and vandalism, as justification for conducting investigations of civil rights, social justice, and environmental activists.[19] These investigative authorities pose a significant threat to speech, association, and religious conduct that is protected under the First Amendment, and the FBI's retention of information gathered through surveillance and investigation conducted pursuant to these authorities erodes the privacy of innocent Americans.

Biased profiling and investigations could be banned through strong agency prohibitions. But even though DOJ's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies purported to ban biased profiling, it created broad exceptions

---

[13] ACLU, Unleashed and Unaccountable: The FBI's Unchecked Abuse of Authority 9–15 (Sept. 2013), https://www.aclu.org/sites/default/files/field_document/unleashed-and-unaccountable-fbi-report.pdf.

[14] *See* Fed. Bureau of Investigation, Domestic Investigations and Operations Guide §§ 4.3.3, 5.1, 6.5–6 (Mar. 2016), https://www.justsecurity.org/wp-content/uploads/2019/03/FBI.DIOG_.pdf.

[15] *See, e.g., id.* at § 4.3.3; *Expanded FBI Authority*, ACLU, https://www.aclu.org/other/expanded-fbi-authority (last visited June 29, 2022) (explaining expanded FBI authorities and recommended reforms).

[16] *See* Press Release, ACLU, Government Linking Various Criminal Behaviors to Certain Racial and Ethnic Groups, Documents Obtained by ACLU Reveal (Oct. 20, 2011), https://www.aclu.org/press-releases/foia-documents-fbi-show-unconstitutional-racial-profiling; ACLU, ACLU Eye on the FBI: The FBI is Engaged in Unconstitutional Racial Profiling and Racial 'Mapping' (Oct. 2011), https://www.aclu.org/aclu-eye-fbi-fbi-engaged-unconstitutional-racial-profiling-and-racial-mapping.

[17] *See generally* ACLU, Unleashed and Unaccountable: The FBI's Unchecked Abuse of Authority (Sept. 2013).

[18] *See* Janet Reitman, *I Helped Destroy People*, N.Y. Times (Sept. 1, 2021), https://www.nytimes.com/2021/09/01/magazine/fbi-terrorism-terry-albury.html.

[19] Office of Inspector Gen., U.S. Dep't of Justice, A Review of the FBI's Investigations of Certain Domestic Advocacy Groups 186 (Sept. 2010); *see also* Press Release, ACLU, New Documents Show FBI Targeting Environmental and Animal Rights Groups Activities as "Domestic Terrorism" (Dec. 20, 2005), https://www.aclu.org/news/new-documents-show-fbi-targeting-environmental-and-animal-rights-groups-activities-domestic.

for national and border security.[20] When DOJ updated this guidance in 2014, it kept these broad loopholes in place, over the objections of communities of color, and civil and human rights organizations nationwide.[21] These loopholes permit racial or religious profiling and violate the stated goals of the Guidance.

DHS similarly allows for bias-based surveillance and investigation in its own non-discrimination guidance. In 2013, DHS issued Guidance to govern law enforcement, investigation, and screening activities.[22] In that Guidance and in subsequent policy, DHS explicitly incorporates both the 2003 and 2014 DOJ Guidance on Race,[23] which exempts DHS's central functions—national and border security—from protections against racial discrimination. Not only does the 2013 DHS Guidance leave these loopholes open, but it contains even more gaps. First, it fails to cover religion, gender and gender identity, and sexual orientation. This is particularly concerning given, for example, DHS's history of disproportionately profiling and watchlisting Muslims.[24] Second, even where certain traits such as race and ethnicity are protected, the DHS Guidance allows consideration of these traits where there is a compelling government interest.[25] This is a significant loophole because DHS often claims that national security, an elastic term and core part of DHS's function, constitutes a compelling government interest and courts have often agreed with this characterization.[26] Finally, the DHS Guidance leaves open the use of national origin

---

[20] U.S. Dep't of Justice, Civ. Rts. Div., Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (June 2003), https://www.justice.gov/sites/default/files/crt/legacy/2010/12/15/guidance_on_race.pdf.

[21] Coalition Letter from the Leadership Conf. on Civ. and Human Rts. to the President Re: Concerns with the U.S. Department of Justice Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (Feb. 24, 2015), https://civilrights.org/resource/re-concerns-with-the-u-s-department-of-justice-guidance-for-federal-law-enforcement-agencies-regarding-the-use-of-race-ethnicity-gender-national-origin-religion-sexual-orientation-or-gender-id; Chris Rickerd, *A Dangerous Precedent: Why Allow Racial Profiling at or Near the Border?,* ACLU (Dec. 8, 2014), https://www.aclu.org/blog/speakeasy/dangerous-precedent-why-allow-racial-profiling-or-near-border.

[22] Memorandum to component heads from Janet Napolitano, Dep't of Homeland Sec., The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities (Apr. 26, 2013), https://www.dhs.gov/sites/default/files/publications/secretary-memo-race-neutrality-2013_0_1.pdf [hereinafter DHS Guidance].

[23] *See, e.g., id.*; U.S. Dep't of Justice, Civ. Rts. Div., Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (June 2003); Dep't of Homeland Sec., Fact Sheet: U.S. Department of Justice Racial Profiling Guidance (Dec. 8, 2014), https://www.dhs.gov/news/2014/12/08/fact-sheet-us-department-justice-racial-profiling-guidance; U.S. Dep't of Justice, Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (Dec. 2014).

[24] Jeremy Scahill & Ryan Devereaux, *Watch Commander: Barack Obama's Secret Terrorist-Tracking System, by The Numbers*, Intercept (Aug. 6, 2014), https://theintercept.com/2014/08/05/watch-commander.

[25] DHS Guidance at 1.

[26] *See* Shirin Sinnar, *Courts Have Been Hiding Behind National Security for Too Long*, Brennan Ctr. for Justice, (Aug. 11, 2021), https://www.brennancenter.org/our-work/analysis-opinion/courts-have-been-hiding-behind-national-security-too-long.

and nationality, permitting profiling in situations where "such consideration is based on an assessment of intelligence and risk."[27] Given the opaque and flawed[28] nature of DHS's risk assessments and methods, this leaves a glaring loophole for profiling on the basis of national origin, which can also be used as a proxy for race, religion, and ethnicity and serve as a pretext for profiling on the basis of otherwise protected traits.[29] These gaps also allow for "Fusion Centers," DHS-supported intelligence-sharing hubs, to share suspicious activity reports (SARs) generated about people engaged in activities loosely labeled as "suspicious" without reasonable suspicion of criminal activity.[30] A 2012 Senate investigation of Fusion Centers found that these reports were "oftentimes shoddy" and "rarely timely."[31] The Senate report also highlighted that Muslim groups were often scrutinized for benign events and routine religious observance under the pretext of counterterrorism.[32] Despite the Senate's investigation, these issues have persisted. In recent years, Fusion Centers have monitored protesters at Standing Rock, people protesting the Trump administration's family separation and border policies, and Black Lives Matter activists.[33]

DHS also purports to address racial profiling through Intelligence Oversight Guidelines which govern the activities of the Office of Intelligence and Analysis (I&A). I&A is a channel between federal and state and local agencies to share counterterrorism information.[34] I&A's Guidelines prohibit "intelligence activities based on *solely* on an

---

[27] DHS Guidance at 2.

[28] Faiza Patel, Rachel Levinson-Waldman & Harsha Panduranga, *A Course Correction for Homeland Security* 10–11, Brennan Ctr. for Justice (Apr. 20, 2022), https://www.brennancenter.org/our-work/research-reports/course-correction-homeland-security [hereinafter Brennan Report].

[29] Faiza Patel, *Trump Administration's Fuzzy Math on Terrorist Origins is More than Misleading – It's Dishonest*, Just Security (Jan. 16, 2018), https://www.justsecurity.org/51084/trump-administrations-fuzzy-math-terrorist-origins-misleading-its-dishonest.

[30] *Gill v. DOJ – Challenge to Government's Suspicious Activity Reporting Program*, ACLU (July 11, 2014), https://www.aclu.org/cases/gill-v-doj-challenge-governments-suspicious-activity-reporting-program.

[31] Federal Support for an Involvement in State and Local Fusion Centers: Permanent Subcomm. on Investigations. of the S. Comm. on Homeland Sec. and Governmental Affairs, 112th Congress 27 (2012), https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

[32] *Id.* at 38.

[33] *See* Alleen Brown, Will Parrish & Alice Speri, *Standing Rock Documents Expose Inner Workings of "Surveillance-Industrial Complex,"* Intercept (June 3, 2017), https://theintercept.com/2017/06/03/standing-rock-documents-expose-inner-workings-of-surveillance-industrial-complex; Ryan Devereaux, *Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests*, Intercept (Apr. 29, 2019), https://theintercept.com/2019/04/29/family-separation-protests-surveillance; 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.

[34] 6 U.S.C. § 121 (2018); *see* Dep't of Homeland Sec., Office of Intelligence and Analysis, Office of Intelligence Oversight Program and Guidelines 3–4 (Jan. 2017) https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf (emphasis added).

individual's or group's race, ethnicity, gender religion, sexual orientation, gender identity, country of birth, or nationality,"[35] but the "sole" limitation is weak and would permit intelligence gathering based on these characteristics combined with neutral and unsubstantiated justifications that may still allow for racial disparities. For example, in March 2022, DHS's inspector general compared I&A's open source intelligence reports in the weeks leading up to the January 6, 2021 events at the U.S. Capitol with the reports issued during racial justice protests during the summer of 2020.[36] There was a stark contrast in the volume and seriousness of the reports issued during these two time frames, with 366 reports issued during the racial justice protests and *zero* reports in the weeks leading up to January 6. While the inspector general's findings did not assess or determine the reasons for this disparity, the difference is striking given I&A's history of disseminating social media information of those protesting the Trump administration's family separation and border policies,[37] and those engaged in political dissent related to police brutality[38] This, combined with DHS's limited prohibitions on racial profiling, creates reason for concern—especially for individuals from marginalized communities seeking to exercise their First Amendment rights.

Recommendation No. 1

The ACLU urges the PCLOB to conduct a case study of FBI assessments that the FBI has identified as related to "domestic terrorism" from 2014 to the present in order to understand how those assessments rely on race, religion, and First Amendment–protected activities—including by sampling investigations involving so-called "Domestic Violent Extremists" and subcategories such as "Racially Motivated Violent Extremists," "Black Separatist Extremists," "Abortion-Related Violent Extremists," white supremacists, religious organizations and adherents, and environmental and social justice activists.

We further urge the PCLOB to conduct a study of I&A's open source intelligence reports (OSIRs) and Fusion Center reports from 2014 to the present to evaluate how reports are generated and how those assessments rely on race, religion, and First Amendment–protected activities. This can be achieved by sampling reports involving so-called "Domestic Violent Extremists" and subcategories such as "Racially Motivated Violent Extremists," "Black Separatist Extremists," "Abortion-Related Violent Extremists,"

---

[35] Dep't of Homeland Sec., Office of Intelligence and Analysis, Office of Intelligence Oversight Program and Guidelines 2–3 (Jan. 2017).

[36] Office of the Inspector Gen., I&A Identified Threats Prior to January 6, 2021, but Did Not Issue Any Intelligence Products Before the U.S. Capitol Breach (Mar. 2022), https://www.oig.dhs.gov/sites/default/files/assets/2022-04/OIG-22-29-Mar22-Redacted.pdf.

[37] Ryan Devereaux, *Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests*, Intercept (Apr. 29, 2019), https://theintercept.com/2019/04/29/family-separation-protests-surveillance.

[38] 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.

white supremacists, religious organizations and adherents, and environmental and social justice activists.

II. Center for Prevention Programs and Partnerships

Last year, DHS announced new measures to address "domestic violent extremism," with a focus on white supremacy, including the creation of the Center for Prevention Programs and Partnerships. However, DHS's efforts come in the shadow of previously harmful programs, discussed above and below, and appear to use similar frameworks and methodologies without clear guidelines, definitions, or safeguards to protect civil rights and civil liberties.

On May 11, 2021, DHS announced the establishment of the Center for Prevention Programs and Partnerships.[39] According to Secretary Mayorkas, CP3 replaces the Office for Targeted Violence and Terrorism Prevention (TVTP) and focuses on "threat assessments" intended to detect "risk factors for radicalization to violence."[40] DHS described this effort as a "whole-of-society" approach, including collaboration across every level of government, the private sector, non-governmental organizations, and communities.[41] However, since this announcement, DHS has released very little information about CP3 and the new domestic terrorism branch. And while DHS states that CP3 is intended to address domestic terrorism and targeted violence, DHS has not publicly released information regarding how it defines those phenomena. Similarly, while CP3 claims to coordinate extensively with the DHS Office for Civil Rights and Civil Liberties (CRCL) in its prevention mission,[42] the public has no information about CRCL's role, how its input factors into CP3's work, and whether and how civil liberties, rights, and privacy are safeguarded.

The lack of publicly available information regarding CP3 is particularly concerning given DHS's history of using flawed counterterrorism frameworks that disproportionately impact communities of color and immigrants. By viewing American communities through the lens of national security, these programs have targeted and harmed Black and Brown people, particularly Muslims, as well as other marginalized communities. For example, the Countering Violent Extremism program created under the Obama administration utilized a deeply flawed approach that called on social service providers and community members to identify potentially "extremist" individuals based on vague and broad criteria that

---

[39] *See* Press Release, Dep't of Homeland Sec., DHS Creates New Center for Prevention Programs and Partnerships and Additional Efforts to Comprehensively Combat Domestic Violent Extremism (May 11, 2021), https://www.dhs.gov/news/2021/05/11/dhs-creates-new-center-prevention-programs-and-partnerships-and-additional-efforts [hereinafter CP3 Press Release].

[40] Dep't of Homeland Sec., Ctr. for Prevention Programs and Partnerships Overview (2022), https://www.dhs.gov/sites/default/files/2022-02/The%20Center%20for%20Prevention%20Programs%20and%20Partnerships.pdf.

[41] *See* CP3 Press Release.

[42] *See* Dep't of Homeland Sec., Center for Prevention Programs and Partnerships Overview (2022).

encompassed lawful speech and association.[43] The Trump administration also adopted this model in creating the TVTP Office, raising the same acute concerns for communities of color and immigrants.[44] CP3 comes in the shadow of these harmful and ineffective programs and appears to use similar frameworks and methods—such as "threat assessments" intended to detect "risk factors for radicalization to violence"—without clear guidelines, definitions, or safeguards to protect civil rights and liberties.[45]

Given the potential impacts CP3 will have on the civil rights, liberties, and privacy of communities of color, immigrants, and other marginalized communities that have already experienced harm under predecessor models, it is imperative that the public gain a greater understanding about the policies, practices, methods, and goals of CP3.

Recommendation No. 2

The ACLU urges the Board to make public key facts about CP3, including how CP3 defines "targeted violence" and "domestic terrorism," and the methodology and frameworks used to identify targeted violence or "radicalization to violence." We further urge PCLOB to assess the program's impact on civil rights, liberties, and privacy, and to recommend appropriate safeguards.

III. Mapping DHS surveillance and information-processing systems

The PCLOB should also engage in a study that comprehensively maps for the first time the many surveillance and information-processing systems DHS uses for counterterrorism purposes, including systems that DHS is deploying or expanding to track and predict "domestic violent extremism."[46] DHS has failed to provide even basic information about the full range of these activities to the public, let alone a clear picture of the relationships between its various systems. The need for such a public accounting is especially urgent as DHS increasingly uses algorithmic or artificial intelligence systems to

[43] *See* Murtaza Hussain, *Federal 'Countering Violent Extremism' Grants Focus on Minority Communities – Including in Schools*, Intercept (Jun. 15, 2018), https://theintercept.com/2018/06/15/cve-grants-muslim-surveillance-brennan-center.

[44] *See* Press Release, DHS, Acting Secretary McAleenan Announces Establishment of DHS Office for Targeted Violence and Terrorism Prevention (Apr. 19, 2019), https://www.dhs.gov/news/2019/04/19/acting-secretary-mcaleenan-announces-establishment-dhs-office-targeted-violence-and.

[45] Dep't of Homeland Sec., Center for Prevention Programs and Partnerships Overview (2022).

[46] *See, e.g.*, Ken Dilanian, *DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media*, NBC News (May 10, 2021), https://www.nbcnews.com/politics/national-security/dhs-launches-warning-systemfind-domestic-terrorism-threats-public-social-n1266707; Rachael Levy, *Homeland Security Considers Outside Firms to Analyze Social Media After Jan. 6 Failure*, Wall St. J. (Aug. 15, 2021), https://www.wsj.com/articles/homeland-security-considers-outside-firms-to -analyze-social-media-after-jan-6-failure-11629025200.

analyze information and guide agency decisions that may have a profound impact on the civil rights and civil liberties of people in the United States.

A. DHS collection and processing of sensitive data

DHS collects vast amounts of information about people in the United States and those seeking to enter the country. Its surveillance tools include social media monitoring; purchases of commercial datasets that can include sensitive location information; collection of biometric information at ports of entry; and the monitoring of passenger travel records, which are then mined to conduct even more intrusive physical and electronic searches when individuals are crossing the border. The resulting data is processed and distributed by a sprawling web of interconnected systems, which inform or guide agency decisions affecting individuals' basic civil rights and civil liberties. As former DHS officials have explained, the Department's collection and use of information about citizens and people traveling to or living in this country raise such significant concerns that "the privacy and due process concerns resulting from other homeland security operations, such as information collection by the National Security Agency, pale by comparison."[47] Although the public gets fleeting, partial glimpses of DHS's surveillance activities through Privacy Impact Assessments and Freedom of Information Act disclosures, there remains immense opacity surrounding what information is collected by DHS and how that information is analyzed and used in practice.

Without this kind of mapping, effective congressional oversight and public accountability will continue to be extremely difficult if not impossible to achieve. Indeed, although the full scope of DHS's activities is unknown, examples of its surveillance and information-processing systems include:

Social media monitoring: In May 2021, DHS launched a social media monitoring program that it claimed would help identify domestic violent extremists and predict future acts of violence.[48] Almost nothing is known about what data sources the program draws on, what standards agents apply in reviewing and analyzing social media posts, or how the resulting information is acted upon by DHS or others. This program operates alongside other social media monitoring programs that Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and United States Citizenship and Immigration Services

[47] Chappell Lawson & Alan Douglas Bersin, *Beyond 9/11: Homeland Security for the Twenty-First Century* 303 (Chappell Lawson et al. eds., 2020).

[48] *See* Ken Dilanian, *DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media*, NBC News (May 10, 2021), https://www.nbcnews.com/politics/national-security/dhs-launches-warning-systemfind-domestic-terrorism-threats-public-social-n1266707; Rachael Levy, *Homeland Security Considers Outside Firms to Analyze Social Media After Jan. 6 Failure*, Wall St. J. (Aug. 15, 2021), https://www.wsj.com/articles/homeland-security-considers-outside-firms-to-analyze-social-media-after-jan-6-failure-11629025200; Ken Dilanian & Julia Ainsley, *DHS weighing major changes to fight domestic extremism, say officials*, NBC News (Mar. 21, 2021), https://www.nbcnews.com/politics/national-security/dhs-weighing-huge-changes-fight-domestic-violent-extremism-say-officials-n1262047 ("The idea is to identify people who may through their social media behavior be prone to influence by toxic messaging spread by foreign governments, terrorists and domestic extremists.").

(USCIS) use to continuously vet individuals who have applied for or received permission to come to the United States for school, work, or other reasons—purportedly in an effort to detect fraud and prevent violence or terrorism.[49] In many cases—such as the Visa Lifecycle Vetting Initiative, the Overstay Lifecycle program, and the Continuous Immigration Vetting program—this monitoring of social media activity appears to continue even after individuals have arrived in the United States.

Purchases of commercial datasets including sensitive location data: In February 2020, The Wall Street Journal reported that DHS, CBP, and ICE were purchasing access to a massive commercial database containing sensitive location data—often derived from people's cell phone apps—and that ICE was relying on this information for border security and immigration enforcement.[50] Subsequent reporting has identified other companies selling access to similar location databases to DHS.[51] In addition, DHS has contracted with companies that compile the water, gas, electricity, phone, or internet utility records of over 150 million Americans,[52] and also with companies that sell access to vast amounts of license plate information.[53]

Collection of biometric information: DHS has long collected sensitive biometrics, including fingerprints, and today it is increasingly exploring the collection of faceprints from both non-citizens and U.S. citizens at ports of entry.[54] In recent years, DHS has also secretly scanned the faces of millions of drivers in the United States and has contracted with a company that indiscriminately scrapes Americans' photos off the internet in order to compile and sell access to a massive faceprint database.[55] The PCLOB has at least one ongoing project

---

[49] *See* Coalition Letter to Secretary Mayorkas Urging an End to Biased Profiling and Seeking Privacy-Protecting Surveillance Reforms (Sept. 15, 2021), https://www.aclu.org/letter/coalition-letter-secretary-mayorkas-urging-end-biased-profiling-and-seeking-privacy; Brennan Report.

[50] Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

[51] Charles Levinson, *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, Protocol (Mar. 5, 2020), https://www.protocol.com/government-buyinglocation-data.

[52] *See, e.g.*, Drew Harwell, *ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations*, Wash. Post (Feb. 26, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data.

[53] Georgetown Center on Technology & Policy, American Dragnet: Data-Driven Deportation in the 21st Century (May 2022), https://americandragnet.org; DHS Privacy Office, Privacy Impact Assessment for the CBP License Plate Reader Technology, DHS/CBP/IA-049(a) (July 2020), https://www.dhs.gov/sites/default/files/publications/ privacy-pia-cbp049a-cbplprtechnology-july2020.pdf.

[54] Although U.S. citizens are not currently required to submit faceprints at ports of entry, many U.S. citizens have had extreme difficulty opting out of CBP's supposedly voluntary face recognition pilot programs. *See* Comment of Civil Society Organizations in Opposition to 85 Fed. Reg. 74162 at 16 (Dec. 21, 2020), https://www.aclu.org/sites/default/files/field_document/comment_re_cbp_face_surveillance_nprm_final.pdf.

[55] Drew Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, Wash. Post (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-

related to facial recognition and other biometric technologies in aviation security, which could contribute to a broader effort to map DHS's collection and use of biometrics.[56]

Homeland Advanced Recognition Technology (HART): DHS is in the process of deploying its HART database as the agency's primary system for storage and processing of biometric and associated biographic information for national security, law enforcement, immigration, border management, intelligence, background investigations, and a number of other uses.[57] When fully deployed, it will replace the prior IDENT system and will support biometrics that include faceprints, fingerprints, voice data, DNA, scars and tattoos, and a blanket category for "other modalities."[58]

Collection of passenger travel records: DHS requires airlines operating flights to, from, or through the United States to provide passenger name records (PNR) data.[59] This data can include vast amounts of information such as identification data, transactional data, financial data, flight information, choice of meal, and data relating to the place of residence.[60] The PCLOB already has an ongoing oversight project related to the use of PNRs, but no information about the project's status or findings has been publicly released yet.[61]

Automated Targeting System (ATS) & ATLAS: A number of existing and proposed DHS systems purport to assess whether an individual poses a "threat" or to predict instances of fraud, violence, or radicalization. At the heart of these systems is the Automated Targeting System (ATS), which relies on secret rule sets and algorithms, in combination with public data such as social media, and can lead to prolonged border detentions, intrusive searches,

---

driverslicense-photos-are-gold-mine-facial-recognition-searches/; Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, Buzzfeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[56] *Projects,* U.S. Privacy and C.L. Oversight Bd., https://www.pclob.gov/Projects (last visited June 23, 2022).

[57] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA (Feb. 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.

[58] 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.

[59] *See* U.S. Customs and Border Protection, Frequently Asked Questions: Receipt of Passenger Name Record Data 2–3 (Sept. 2019), https://www.cbp.gov/sites/ default/files/assets/documents/2020-May/PNR-FAQs-%28508 -compliant%29.pdf.

[60] Article 29 Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States (Oct. 2002), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp66_en.pdf.

[61] *Projects*, U.S. Privacy and C.L. Oversight Bd.

and unexplained visa denials.[62] DHS components utilize ATS for programs like ATLAS and Continuous Immigration Vetting (CIV) to conduct risk assessments of travelers, identify potential instances of immigration fraud, or pursue denaturalization cases, among other applications.[63]

***TECS (formerly the Treasury Enforcement Communications System)*:** TECS is a database and information-sharing system owned and operated by CBP. Using TECS, border officers may "document an observation relating to an encounter with a traveler, a memorable event, or noteworthy item of information particularly when they observe behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention." [64] In addition, border officers record every secondary inspection at an airport or land crossing in TECS, regardless of the outcome of the inspection. The information in TECS is made widely available to law enforcement agencies, including personnel from CBP and other DHS agencies, as well as outside federal, state, local, tribal, and foreign law enforcement, counterterrorism, and border security agencies. Data is retained for up to 75 years.[65] Notably, a 2021 OIG report found that CBP officers flagged individuals in the TECS system where there was no evidence of direct involvement in criminal activities. Through litigation, the ACLU is currently seeking expungement of records, including those stored in TECS, concerning the unlawful questioning of journalists about their work documenting conditions at the U.S.-Mexico border; and, through a separate suit, the expungement of TECS records concerning the unlawful questioning of Muslim Americans at the border about their religious beliefs, practices, and associations.[66]

***National Vetting Center (NVC)*:** NVC is an interagency effort established in 2018 to share intelligence and coordinate vetting operations for individuals seeking to enter the United Sates or apply for immigration-related benefits.[67] According to NVC's implementation plan and a 2018 Privacy Impact Assessment, NVC does not include any independent

---

[62] U.S. Dep't of Homeland Sec., Privacy Impact Assessment Update for the Automated Targeting System (Jan. 2017), https://www.dhs.gov/sites/default/files/2022-05/privacy-pia-cbp006%28e%29-ats-may2022.pdf.

[63] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the ATLAS (Oct. 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis084-atlas-july2021.pdf; Dep't of Homeland Sec., Privacy Impact Assessment for the Continuous Immigration Vetting (Feb. 2019), https://www.dhs.gov/sites/default/files/publications/pia-uscis-fdnsciv-february2019_0.pdf.

[64] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing (Dec. 2010), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf.

[65] *Id.* at 14.

[66] *See Guan v. Mayorkas,* ACLU, https://www.aclu.org/cases/guan-v-wolf (last visited June 30, 2022); *Kariye v. Mayorkas,* ACLU, https://www.aclu.org/cases/kariye-v-mayorkas (last visited June 30, 2022).

[67] *National Vetting Center,* Customs and Border Protection, https://www.cbp.gov/border-security/ports-entry/national-vetting-center (last modified Sept. 28, 2021).

monitoring, audits, limits on information sharing, or internal redress systems.[68] NVC's implementation plan is heavily redacted with respect to its "Phase Two" efforts, leaving the public in the dark about the NVC's plans for the future.[69]

B. DHS adoption and use of artificial intelligence

The lack of transparency described above has been compounded by DHS's adoption of artificial intelligence (AI) systems with virtually no public input or oversight. Yet these systems also pose undeniable risks to civil rights and civil liberties. In March 2021, the National Security Commission on Artificial Intelligence (NSCAI) signaled that DHS (and the FBI) had already taken significant steps to develop and field artificial intelligence systems. Echoing many of the concerns raised about "black box" systems like ATS and ATLAS, the Commission warned that DHS "must take care to ensure that automated screening processes lead agents only to the information they need and are authorized to access, and do not impermissibly single out individuals based on characteristics such as race or religion."[70]

More broadly, DHS's secret development and use of AI tools raises urgent concerns about whether these new systems are biased against people of color and marginalized communities, and whether they are being used to automate or legitimize discriminatory government conduct. AI systems may replicate biases embedded in the data used to train those systems,[71] and they may have higher error rates when applied to people of color, women, and marginalized communities because of other flaws in the underlying data or in the algorithms themselves.[72] In addition, AI may be deployed to expand government activities that have long been used to unfairly and wrongly scrutinize communities of color—including intrusive surveillance, investigative questioning, detention, and watchlisting.

Based on its study, the NSCAI recommended that DHS (and the FBI) impose new obligations for System of Record Notices (SORNs) and Privacy Impact Assessments (PIAs) specific to AI systems to ensure that they provide vital information to the public. It noted

---

[68] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the National Vetting Center (Dec. 2018), https://www.dhs.gov/sites/default/files/2022-05/privacy-pia-dhsall072-nvc-may2022v2.pdf.

[69] Nat'l Vetting Ctr., Plan to Implement the Presidential Memorandum on Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise (Aug. 2018), https://www.dhs.gov/sites/default/files/publications/NSPM-9%20Implementation%20Plan.pdf.

[70] Nat'l Sec. Comm'n on A.I., Final Report 145 (2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf [hereinafter NSCIAI Final Report].

[71] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[72] Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News Office (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

that "agency practices do not sufficiently support the production of SORNs and PIAs that adequately depict how AI systems collect, use, and store personal information."[73] The report made three specific recommendations, which echo many of the broader deficiencies in DHS's public disclosures about its surveillance and information-processing systems:

(1) SORNs and PIAs should provide a holistic picture about the collection, use, and storage of personal information by any AI system, including its connections to existing systems and accounting for the layering of different surveillance technologies where applicable.

(2) PIAs should include description of the algorithm(s) used and the purpose of the algorithm(s); the potential for inferring additional information about individuals from the aggregation of multiple data sources; and importantly, the measures that will be used to address these risks.

(3) SORNs should provide more specificity in describing types of data collected, data sources and the connections between data sources, and who will use such data and why.[74]

Beyond these recommendations, DHS's AI and other predictive tools should be subjected to civil rights impact assessments that are made available to the public. These assessments should, at a minimum, include regular evaluation for discriminatory impact based on race or other protected characteristics during the design, development and after deployment of any AI or other predictive model; proactive searches for and adoption of less discriminatory alternatives; continuing assessments of whether the data used in training technologies is representative and accurate; and assessments of whether the technologies measure lawful and meaningful attributes and seek to predict valid target outcomes.

To date, DHS's disclosures about its use of AI have not remotely met these basic requirements for meaningful public input and oversight. As part of a broader mapping of DHS systems, the PCLOB should ensure that this critical information about DHS's deployment of AI reaches the public.

Recommendation No. 3

We urge the Board to conduct a study and make public a report describing (1) the various kinds of information collected by DHS for counterterrorism purposes; (2) the legal authority for collection and retention; (3) the purposes for which the information is used; (4) how it flows within DHS and to other agencies and foreign governments; (5) what algorithmic or artificial intelligence systems are used to collect or analyze data, and to

[73] NSCAI Final Report at 397.

[74] *Id.*

guide or make decisions based on that information; and (6) the impact of DHS's collection, dissemination, and analytical tools on civil rights and liberties.

* * *

For more information, please contact Sana Mayat at smayat@aclu.org or 212.549.2500.

Sincerely,

/s/ Sana Mayat
Sana Mayat, Nadine Strossen Fellow
Hina Shamsi, Project Director
Patrick Toomey, Senior Staff Attorney
Ashley Gorski, Senior Staff Attorney
Brett Max Kaufman, Senior Staff Attorney
National Security Project
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
smayat@aclu.org
212.549.2500