July 1, 2024

Privacy and Civil Liberties Oversight Board
800 North Capitol Street, N.W.
Washington, DC 20002

Comment of the American Civil Liberties Union and the Brennan Center for Justice for the PCLOB Public Forum on Artificial Intelligence in Counterterrorism and Related National Security Programs

Dear Privacy and Civil Liberties Oversight Board Members,

The American Civil Liberties Union (ACLU) and the Brennan Center for Justice at NYU School of Law (Brennan Center) are pleased to provide this comment regarding the Privacy and Civil Liberties Oversight Board's (PCLOB or the Board) upcoming public forum on "the role of artificial intelligence (AI) in counterterrorism and related national security programs, and privacy and civil liberties issues associated with these uses of AI."[1]

Introduction

The use of AI for counterterrorism purposes is an area in urgent need of the Board's oversight. National security agencies—including those with law enforcement, intelligence, homeland security, and defense components—have long relied on AI systems and are rapidly expanding their use, presenting immense risks to the rights and safety of people in the United States and abroad. While Congress and the Biden administration have taken steps to increase transparency, trust, and fairness in the AI tools used by many federal agencies, national security agencies have been largely exempted from these developments. The Board should use its oversight authority to address this considerable gap—by conducting deep-dive examinations of some of the most pressing uses of AI related to counterterrorism, by publicly reporting on the results of those reviews, and by recommending safeguards commensurate with the risks posed by these novel technologies. Those safeguards should include, where necessary, calling for a halt on the use of any AI system that the Board determines has not been sufficiently tested, is unreliable, or raises intolerable risks for civil liberties, civil rights, or safety.

Today, U.S. national security agencies and the military are seeking to integrate AI into some of the government's most profound decisions: who it surveils, who it places on government watchlists, who it subjects to intrusive searches at the border, who it labels a "risk" or "threat" to national security, and even who or what it targets with lethal force.[2] All of these AI-powered decisions connect, in some way, to the government's wide-ranging counterterrorism efforts—though the same tools may often be used to pursue broader national security and law enforcement purposes as well. These programs—even without AI augmentation—have not been meaningfully tested for efficacy and are characterized by

[1] PCLOB, Notice & Request for Public Comment, 89 Fed. Reg. 45711, Notice-PCLOB-2024-01 (May 23, 2024) (here).

[2] *See, e.g.*, Nat'l Sec. Comm'n on A.I. (NSCAI), *Final Report* 143–45 (2021) (here) [hereinafter NSCAI Final Report].

vague and overbroad standards, weak safeguards, and little to no transparency. Yet rather than fix these fundamental flaws before expanding the programs, in many areas, the real-world deployment of AI appears to be well underway.

While the rushed adoption of AI poses risks in many contexts, the use of AI for counterterrorism and related national security activities presents some of the greatest dangers to people in the United States and abroad. The deployment of AI systems for surveillance, watchlisting, border searches, biometric identification, and immigration vetting will automate, expand, and make even more opaque some of the government's most intrusive, damaging, and secretive programs. Moreover, these programs and activities disproportionately impact communities that have long faced bias and discrimination, such as immigrants and racial and religious minorities. As in areas like policing and the criminal legal system, the use of AI for counterterrorism purposes could easily perpetuate racial, ethnic, or religious profiling, while broadly endangering civil rights and civil liberties.

Despite these dangers, both transparency and accountability safeguards are severely lacking—and, to the extent they exist at all, largely unenforceable. The public knows little about the AI being deployed by the country's largest intelligence, homeland security, and law enforcement entities like the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Central Intelligence Agency (CIA). And the public knows even less about the civil rights and liberties protections that exist—if any. National security agencies have embarked on an all-out sprint to develop and deploy AI, but any efforts to protect civil rights and civil liberties have been slow-moving and today lack meaningful transparency and binding rules. For example, the Office of the Director of National Intelligence's (ODNI) *Principles for Artificial Intelligence Ethics for the Intelligence Community* describes six high-level guidelines—including a commitment to be "transparent and accountable"—but the public to date has seen little evidence of either.[3] The Department of Defense (DOD) last year released a toolkit "to help DOD personnel design, develop, deploy, and use AI systems responsibly," but using the toolkit is voluntary.[4] DHS has issued a policy statement pledging transparency and "particular attention to continued Component participation in the AI Use Case Inventory process," but the Government Accountability Office found as recently as February 2024 that its inventory is incomplete.[5]

Most notably, the executive branch's flagship effort to regulate the use of AI by federal agencies—the recent guidance memo issued by the Office of Management and Budget (OMB Memo M-24-10)—exempts "national security systems" from its rules

[3] ODNI, *Intelligence Community Principles of Artificial Intelligence* (2020) (here); ODNI, *Artificial Intelligence Ethics Framework for the Intelligence Community* (June 2020) (here).

[4] DOD, *CDAO Releases Responsible AI (RAI) Toolkit for Ensuring Alignment with RAI Best Practices* (Nov. 14, 2023) (here).

[5] DHS, *Policy Statement 139-06 on the Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components* at 2 (Aug. 8, 2023) (here); Government Accountability Office (GAO), *Artificial Intelligence: Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity* (GAO-24-106246) (Feb. 2024) (here).

altogether.[6] President Biden's executive order on AI (EO 14110) requires a separate National Security Memorandum that the administration will release in the coming months.[7] But the exemptions, carve-outs, and waivers in OMB Memo M-24-10 raise the specter of a two-tiered approach that contains only weak protections when it comes to national security uses, including counterterrorism.[8]

Given these severe transparency and oversight gaps, PCLOB should conduct a searching review of the AI tools falling within its mandate, and publicly issue forceful conclusions about those tools' impact on privacy and civil liberties. There is currently no other executive branch mechanism for independent scrutiny of AI systems used by national security agencies.[9] Counterterrorism activities that rely on AI are simply too high stakes for people in the United States to be left solely to unaccountable and opaque internal executive branch oversight mechanisms.[10]

The Board should also define the scope of its review broadly, to encompass algorithmic decision-making systems that may be less complex than state-of-the-art machine learning systems but no less dangerous. For example, DHS's Automated Targeting System (ATS), described below, relies on secret "targeting rules" to assess whether individuals pose a "threat" to national security, and can lead to prolonged border detentions, intrusive searches, and unexplained visa denials. ATS and its associated systems run afoul of virtually every pillar for safe, effective, equitable, transparent, and fair algorithmic systems, including the principles laid out in the White House's Blueprint for an AI Bill of Rights.[11] Whether DHS has sought to incorporate artificial intelligence into ATS is not publicly known today, but regardless, it is the kind of opaque algorithmic system that warrants the Board's attention.

As the Board assesses the government's use of AI related to counterterrorism activities, we urge it to do deep-dive investigations and public reporting in at least five domains:

1. The use of AI by national security agencies to collect and analyze private communications, social media information, and other sensitive data;
2. The use of AI by DHS and FBI to screen travelers and immigrants;

---

[6] The exemption was first established by EO 14110. OMB, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (Mar. 28, 2024) (here).

[7] White House, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, Exec. Ord. No. 14110, 88 Fed. Reg. 210 § 10.1 (October 30, 2023) (here).

[8] *See* ACLU, *Comment re: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum* (Dec. 5, 2023) (here); Brennan Center for Justice, *Comment re: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum* (Jan. 8, 2024) (here).

[9] *See* Faiza Patel and Patrick Toomey, *An Oversight Model for AI in National Security: The Privacy and Civil Liberties Oversight Board*, Just Security (Apr. 26, 2024) (here).

[10] *See* Amos Toh and Ivey Dyson, *The Nuts and Bolts of Enforcing AI Guardrails*, Just Security (May 30, 2024) (here).

[11] Rachel Levinson-Waldman and José Guillermo Gutiérrez, *DHS Must Evaluate and Overhaul its Flawed Automated Systems*, Just Security (Oct. 19, 2023) (here).

3. The use of AI for facial recognition;
4. The use of AI by the Department of Defense to identify or recommend targets for lethal strikes; and
5. The use of AI by DHS to protect "soft targets" in the United States.

These use cases—and any other use of AI in highly consequential counterterrorism programs—should incorporate the bedrock principles articulated in EO 14110 and OMB Memo M-24-10. This means finding avenues for transparency in areas that are traditionally secret; developing mechanisms for assuring the public that AI tools are effective, lawful, free from bias, and preserve privacy; ensuring due process and an opportunity for redress; and establishing robust oversight and governance mechanisms.

In particular, we urge the Board to recommend the following safeguards for the AI systems that come within its mandate:

- Increased transparency across all such systems, through the development of comprehensive AI use case inventories, regular declassification reviews, and improvements in existing transparency reporting.
- Adoption of risk management practices that reduce or prevent harm to privacy and civil liberties, including impact assessments, real-world testing, and ongoing risk monitoring protocols.
- Increased scrutiny and oversight of whether and to what extent AI has been effective at accomplishing the agency's counterterrorism or national security objectives, such as through meaningful gains in the accuracy of detecting or preventing terrorism activities.
- A minimum standard requiring agencies to refrain from or cease AI use when: (1) the AI is not sufficiently tested; (2) it is unreliable or otherwise ineffective; or (3) it raises risks to privacy, civil liberties, civil rights, or safety that cannot be effectively mitigated.
- Increased resources and support for agencies' internal oversight mechanisms to scrutinize and ensure compliance with AI-related safeguards.

Given the Board's independence and its expertise, we believe it must play a central role in ensuring accountability amidst the federal government's rush to bring AI into some of its most consequential activities. Below we set forth our key concerns and recommendations.

The AI Transparency Deficit and Recommendations

Our analysis of the current state of AI in counterterrorism and related national security systems below draws largely on information obtained from media reports, leaked documents, and Freedom of Information Act requests. The lack of proactive and meaningful disclosures from the federal government makes it nearly impossible for the public to understand how AI systems are used in these operations, how these systems make decisions or recommendations, how their outputs influence agency decisions or action, and what safeguards, if any, are in place. Obscuring these basic facts stifles public discourse

about the appropriate role of AI in counterterrorism, whether the technology is effective at accomplishing its stated goals, and the technology's role in facilitating abusive or unconstitutional practices.

People directly affected by counterterrorism AI are also prevented from seeking redress for violations of their privacy, civil liberties, and civil rights. For example, while Americans on the government's No Fly List may receive confirmation of their status on it, the government can withhold its reasons and evidence for placement on national security and law enforcement grounds.[12] This makes it extremely difficult, if not impossible, for affected travelers to challenge wrongful placement on the list—including the role of AI in the process. The government refuses to provide travelers on other government watch lists, or those who have been flagged by risk prediction systems for additional searches and questioning at the border, with even this basic information.[13]

While Congress and the White House have begun to require agencies to report and disclose how they are using AI, they have established sweeping carveouts for national security applications of the technology. The Advancing American AI Act of 2022 exempts the Intelligence Community (IC) and DOD from its requirement to publish AI use case inventories.[14] EO 14110 exempts AI "used as a component of a National Security System" from the OMB's March 2024 guidance imposing guardrails on agency use of AI.[15] National security AI is to be governed by a separate and forthcoming National Security Memo (NSM), which may contain weaker safeguards.[16] It is unclear whether the NSM will incorporate key transparency measures outlined in OMB Memo M-24-10, such as use case inventories, and requirements for agencies to consult and incorporate feedback from affected communities and the public on their use of AI, and to notify individuals negatively affected by such use. There is also little clarity on which set of rules would apply to systems that serve both national security and non-national security functions, such as social media monitoring tools used to collect domestic intelligence and initiate criminal investigations.

These broad loopholes amplify the government's longstanding practice of cloaking counterterrorism operations in excessive secrecy. To bring meaningful transparency to these highly consequential uses of AI, PCLOB should:

Develop a comprehensive inventory of relevant AI systems. PCLOB should catalog the full range of AI systems used in counterterrorism and related national security operations, their classification markings, which systems have been designated as "national security systems," and the reasons for such designation. This inventory should also include essential information about the intended purpose(s) of these systems, how they work (e.g. a summary of training data used, categories of data inputs and outputs, model parameters), and applicable safeguards (e.g. privacy protections, impact assessments, risk mitigation

---

[12] Rachel Levinson-Waldman and Jose Gutierrez, *Overdue Scrutiny for Watch Listing and Risk Prediction,* Brennan Center for Justice at 4–5 (Oct. 19, 2023) (here) [hereinafter *Overdue Scrutiny*].

[13] *Id.*

[14] Advancing American AI Act, Pub. L. No. 117-263, title LXXII, subtitle B, §§ 7225(d), 7228 (2022) (exempting the Department of Defense and the intelligence community) (here).

[15] OMB Memo M-24-10, § 3(a)(iv).

[16] *Id.* § 2(c); EO 14110.

measures). PCLOB should also document whether these systems are used for non-national security purposes, such as law enforcement or immigration.

PCLOB should make public all information and analysis regarding unclassified AI systems and publish the rest of the inventory to the fullest extent possible. Based on this inventory, PCLOB should report on how agencies are interpreting the definition of a "national security system," and whether additional safeguards are activated when these are used for non-national security purposes.

Urge declassification review. Lawmakers, former government officials, good government advocates, and even the current Director of National Intelligence have concluded that the government routinely overclassifies national security information.[17] Some estimates indicate that 50–90% of classified documents can be safely disclosed to the public.[18]

PCLOB should work with national security agencies and DOD to review whether classified information about their AI systems should be declassified. This review should cover key documentation such as impact assessments, efficacy studies, and measures to monitor and mitigate risks to privacy, civil liberties, and civil rights. For properly classified AI systems, PCLOB should urge system-level disclosures, such as the existence of the system, its general purpose, how it generally works, its anticipated and actual impacts on the privacy and constitutional rights of people in the United States, and general rules and legal analyses governing the system's use.

Recommend improvements to transparency reporting. Existing mechanisms for public reporting on agencies' privacy and data practices should be adapted to increase transparency about how agencies are using AI. DHS and the FBI, for example, are required to publish Privacy Impact Assessments (PIAs) and System of Record Notices (SORNs) that provide information about electronic systems and programs that handle sensitive and personal data, and their compliance with privacy laws, regulations, and policies.[19] But such reporting is all too frequently delayed or skipped, missing critical information, and fragmented in ways that hinder public understanding of complex and interconnected systems.[20] Far more numerous—but not made public—are DHS's privacy threshold

---

[17] *See,* Kai McNamee et al., *The U.S. Has an Overclassification Problem, Says One Former Special Counsel*, NPR (Jan. 17, 2023) (here); CSPAN, *Director of National Intelligence Haines on Classified Information* (Jan. 26, 2023) (here); House Oversight Committee, *Examining the Costs of Overclassification on Transparency and* Security (Dec. 7, 2016) (here); Senate Homeland Security and Governmental Affairs Committee, *Modernizing the Government's Classification System* (Mar. 23, 2023) (here).

[18] Elizabeth Goitein, *The Original Sin Is We Classify Too Much,* Brennan Center for Justice (Jan. 26, 2023) (here).

[19] DHS, *Privacy Impact Assessments* (updated Dec. 1, 2023) (here); DHS, *System of Records Notices (SORNs),* (updated June 24, 2024) (here); FBI, *Department of Justice/FBI Privacy Impact Assessments (PIAs)* (visited July 1, 2024) (here); FBI, *FBI Privacy Act Systems* (visited July 1, 2024) (here).

[20] *See* Spencer Reynolds and Alia Shahzad, *Holding Homeland Security Accountable,* Brennan Center for Justice at 4 (Oct. 26, 2023) (here); Faiza Patel, Rachel Levinson-Waldman, and Harsha Panduranga, *A Course Correction for Homeland Security,* Brennan Center for Justice (Apr. 20, 2022) (here); and Faiza Patel and Patrick Toomey, *Bringing Transparency to National Security Uses of Artificial Intelligence,* Just Security (Apr. 4, 2024) (here).

analyses (PTAs), which provide an initial determination about the privacy implications of a vast array of DHS operations.[21]

PCLOB should urge agencies to specify in PTAs, PIAs and SORNs how their AI systems collect, aggregate, analyze, infer, and retain sensitive and personal data, the personnel granted access to this data, connections between relevant AI systems, and the measures established to monitor and mitigate risks to privacy.[22] This privacy documentation should be hosted in a central online repository that is easily accessible to the public.

AI Use Cases Related to Counterterrorism Activities

1. Use of AI for Intelligence Collection and Analysis

1.1 Intelligence targeting, identification, and analysis

Almost three years ago, the National Security Commission on Artificial Intelligence (NSCAI) issued a sweeping report that made clear that U.S. intelligence and law enforcement agencies like the NSA, CIA, FBI, and others are pursuing "ubiquitous AI integration in each stage of the intelligence lifecycle."[23] Intelligence agencies are seeking to use AI to help select surveillance targets, identify people whose communications are intercepted, and analyze the vast amounts of data they collect.[24] Despite transparency commitments by ODNI and the agencies it oversees, the public knows little about how these AI applications are impacting people in the United States. PCLOB should examine how U.S. national security agencies are using AI to gather and process sensitive information in connection with counterterrorism activities, as well as the safeguards that exist, if any.

The NSA is a case in point, though it is not alone. Among U.S. intelligence agencies, the NSA is the self-described leader in the race to develop and deploy AI.[25] According to officials, the NSA has used AI "for a very long time" to support its intelligence-gathering activities, and today it is one of many spy agencies seeking to integrate AI across its activities.[26] Yet the public knows very little about how exactly the agency is harnessing AI. NSA officials have publicly described the agency's use of AI tools to detect threats to critical infrastructure, to summarize large amounts of information or raw intelligence, and to perform "speaker identification and speech-to-text processing."[27] The NSA likely also uses these tools to select new surveillance targets and to analyze the vast amounts of

---

[21] Reynolds and Shahzad, *Holding Homeland Security Accountable*.

[22] Nat'l Sec. Comm'n on A.I., *Final Report* at 399 (March 2023) (here).

[23] NSCAI Final Report at 110 (here).

[24] *Id.* at 108–10, 143–45.

[25] National Security Agency/Central Security Service, *Our Mission* (visited July 1, 2024) (here).

[26] NSA, *GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT* (Sep. 21, 2023) (here).

[27] *Artificial Intelligence: Next Frontier is Cybersecurity*, NSA.gov (July 23, 2021) (here); Jay Stanley, *Will ChatGPT Revolutionize Surveillance?*, ACLU (Apr. 19, 2023) (here); *An Interview with Paul M. Nakasone*, Joint Force Quarterly, 92 at 4 (Jan. 2019) (here); Justin Doubleday, *NSA Working on New AI 'Roadmap' as Intel Agencies Grapple with Recent Advances*, Federal News Network (July 14, 2023) (here); Matt Kapko, *3 Areas of Generative AI the NSA Is Watching in Cybersecurity*, Cybersecurity Dive (May 1, 2023) (here); Carolyn Shapiro, *The Intelligence Community Is Developing New Uses for AI*, FedTech (Oct. 4, 2022) (here).

communications it collects every day—often ensnaring people in the United States.[28] Indeed, although the NSA generally seeks to collect foreign intelligence, the mass surveillance it conducts under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and other authorities like Executive Order 12333 (EO 12333) routinely sweeps up the sensitive communications and data of Americans.[29]

The NSA is likely experimenting with, and deploying, AI under EO 12333.[30] "The primary source of the NSA's foreign intelligence-gathering authority,"[31] EO 12333 affords agencies wide latitude to conduct surveillance with few meaningful safeguards—including the bulk collection of communications and other sensitive data like location information.[32] Because EO 12333 surveillance is so permissive and generally has no judicial oversight, it is a likely umbrella for the NSA's efforts to integrate novel AI technologies into its intelligence-gathering activities. For example, the NSA may be using AI to automate the "tasking" or target-selection process for surveillance—that is, allowing machine-learning tools to recommend or even automatically initiate surveillance on new targets.[33] If so, nothing whatsoever is known about how the NSA ensures that these AI-chosen targets comply with EO 12333 itself or the NSA's own targeting rules, such as restrictions on targeting people in the United States. For example, where those rules require a "reasonable belief" as to the targeted person's citizenship, location, or other status, how does an AI or machine-learning system decide whether that threshold has been met?[34] Questions about accuracy, compliance with foundational privacy rules, and the role of human review are not addressed by the existing public information.

Purchases of sensitive data may also be fueling the expansion of AI tools within agencies like the NSA. Under authorities like EO 12333, intelligence agencies buy immense quantities of sensitive information from data brokers, including location information, web-browsing records, and mobile app data.[35] Although these purchases generally seek the data of people abroad, they often sweep up highly sensitive information about Americans as well.

---

[28] *See* NSCAI Final Report at 108–18.

[29] *See, e.g.*, Faiza Patel, Elizabeth Goitein, and Amos Toh, *Overseas Surveillance in an Interconnected World*, Brennan Center for Justice (Mar. 16, 2016) (here); Dustin Volz, *FBI Conducted Potentially Millions of Searches of Americans' Data Last Year, Report Says*, Wall Street J. (Apr. 29, 2022) (here).

[30] The NSA is likely also deploying AI under Section 702 of the Foreign Intelligence Surveillance Act, but the full scope of their AI use in this context is also unclear. In an April 2023 opinion, the Foreign Intelligence Surveillance Court noted that the NSA has automated the processing and searching of Section 702-acquired data, and that it was possible the NSA could soon be automating the analysis of such data to identify travelers for heightened scrutiny without human inspection. *See* Memorandum Opinion and Order at 34–40 (FISA Ct. Apr. 11, 2023) (here).

[31] NSA, *Overview of Signals Intelligence Authorities* (Jan. 8, 2007) (here).

[32] *See* Letter from American Civil Liberties Union to PCLOB Members (Jan. 13, 2016) (here).

[33] *See* NSCAI Final Report at 109, 112.

[34] DOD Manual 5240.01, Procedures Governing the Conduct of DOD Intelligence Activities (Aug. 8, 2016) (here).

[35] *See generally* ODNI Senior Advisory Group, *Report to the Director of National Intelligence* (Jan. 27, 2022) (here) (describing the intelligence community's increasing reliance on commercially available information and the dangers it poses for American civil rights and civil liberties); *see also* Emile Ayoub, *Assessing the Intelligence Community's Policy Framework for Commercially Available Information*, Just Security (May 24, 2024) (here).

If AI development and adoption is feeding massive demand for commercially available information within intelligence agencies—for instance, to train AI models—that will only compound the problem, putting even more of Americans' private data in the government's hands. The problem is two-fold. First, that training data may be repurposed and exploited in intelligence investigations without meeting the basic requirements of the Fourth Amendment. Second, AI systems trained on this sensitive data may be capable of drawing conclusions about Americans' private lives in ways that risk abuse and broadly endanger privacy and civil liberties.

The intelligence agencies' secrecy around their use of AI is at odds with their public commitments to transparency. ODNI, which oversees the NSA and more than a dozen other intelligence agencies, has touted transparency as a core principle in its *Artificial Intelligence Ethics Framework for the Intelligence Community*.[36] Yet ODNI and the agencies have provided strikingly little information to the public about the AI systems they are deploying to conduct surveillance and analyze vast amounts of private data. Indeed, while agencies like the NSA have publicly lauded their completion of strategic studies, roadmaps, and congressionally-mandated plans on the integration of AI into their activities,[37] none of those documents have been released to the public, not even in redacted form.[38] The little we do know comes from the Inspector General's semi-annual reports to Congress, which only validate our concerns: the NSA has "areas of improvement" when it comes to "developing, implementing, and communicating requirements on documenting AI tools."[39]

This lack of transparency is especially concerning given the danger that many AI-powered intelligence systems pose for people's civil rights and civil liberties. Just as in areas like law enforcement, using algorithmic systems to gather and analyze intelligence can compound privacy intrusions and perpetuate discrimination. AI systems may be scaling the use of discriminatory or bias-based criteria for intelligence gathering under the guise of statistical objectivity. They may further amplify biases that are embedded in the datasets used to train those systems, and they may have higher error rates when applied to people of color and marginalized communities because of flaws in the algorithms or underlying data. As a result, AI-driven surveillance may be used to guide or expand government activities that have long been used to unfairly scrutinize individuals and communities of color, exposing their lives to wide-ranging government scrutiny under FISA or EO 12333. Yet little is known about the efficacy of the NSA's AI tools, or what safeguards for civil rights and civil liberties are in place.

AI tools have the potential to expand the intelligence community's surveillance dragnet more than ever before, expose private facts about our lives through vast data-mining

---

[36] ODNI, *A.I. Ethics Framework for the Intel. Community, Version 1.0*, Intel.gov (2020) (here).

[37] *See, e.g.*, Lauren C. Williams, *NSA 'Recently Completed' AI Strategic Study, Director Says*, Defense One (Sept. 6, 2023) (here); Martin Matishak, *NSA, Cyber Command Recently Wrapped Studies on AI Use, Director Says*, The Record (Sept. 5, 2023) (here).

[38] The ACLU filed a request under the Freedom of Information Act seeking the release of recently completed studies, roadmaps, and reports that show how the NSA is using AI and how those tools affect people's privacy and civil liberties. *See* ACLU v. NSA – *FOIA Lawsuit Seeking Records About the NSA's Use of Artificial Intelligence*, ACLU (visited July 1, 2024) (here).

[39] NSA OIG, *Semi-Annual Report to Congress, 1 October 2022 to 31 March 2023* at 4 (2023) (here).

activities, and automate decisions that once relied on human expertise and judgment. These are dangerous and powerful tools, as the intelligence agencies' own ethical principles recognize. Still, those agencies have largely left the public in the dark about how this technology is being used and what safeguards, if any, exist.

PCLOB should use its independent oversight authority to evaluate how intelligence agencies are deploying AI, and if necessary, call for a halt to uses that pose unacceptable risks to American civil rights and civil liberties. Without urgent intervention, the intelligence agencies risk failing their own ethical standards: rapidly deploying powerful AI systems without public accountability or oversight.

1.2 Social media monitoring

The FBI, DHS, and the State Department have publicly disclosed that they engage in social media monitoring, including for various counterterrorism purposes like broad-scale threat detection and screening of immigrants and travelers. Other federal agencies with intelligence components may also be conducting this surveillance in secret. Promotional materials from Babel Street, a government contractor for social media monitoring, claim that "84% of U.S. National Security Agencies have partnered with [the company]."[40] Government procurement records indicate that, in addition to the FBI, DHS, and the State Department, Babel Street has sold its software to the Defense Information Systems Agency (DISA), the U.S. Coast Guard, the Navy, the Air Force, the Army, Special Operations Command, and the U.S. Marshals Service.[41]

Based on public descriptions of social media monitoring tools, the FBI, DHS, and the State Department have integrated AI capabilities like "sentiment analysis" and "predictive analytics" into their social media surveillance:

FBI. In March 2022, the FBI purchased 5,000 licenses to use Babel X, a social media monitoring platform created by Babel Street. Babel X enables the Bureau to perform sentiment and emotion analysis to "determine likely attitudes of the targets."[42] The Bureau's procurement records also list "predictive analytics" as a desired (though not required) capability, which it defines as "the ability to project the likely future trends based on the current state of the data."[43] The capabilities Babel Street offers that fit this description include: notifications that provide law enforcement with "situational awareness" of "emerging threats," an open-source intelligence functionality that identifies "foreign threats," and a data synthesis tool that maps social networks that amplify criminal and terrorist activity.[44]

---

[40] Babel Street, *OSINT & Threat Intelligence Software* (visited July 1, 2024) (here).

[41] Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees*, VICE (May 17, 2023) (here).

[42] Department of Justice, *Request for Proposals - Social Media Exploitation - Amendment* 2 (visited July 1, 2024) (here).

[43] *Id*.

[44] *See* Babel Street, *AI-powered Law Enforcement Intelligence* (visited July 1, 2024) (here); Babel Street, *OSINT & Threat Intelligence Software* (visited July 1, 2024) (here); Babel Street, *Understanding Babel Street Synthesis* (visited July 1, 2024) (here).

DHS. U.S. Customs and Border Protection (CBP) has acquired access to Babel X to investigate travelers, immigrants, and "persons of interest;" the Transportation Security Administration (TSA) apparently also has access.[45] Immigration and Customs Enforcement (ICE) monitors a broad swath of social media.[46] Procurement records indicate that, since September 2022, ICE has licensed software from Cobwebs America Inc., a provider of "AI-Powered Open-Source Intelligence" that includes social media analysis.[47]

State Department. Procurement records indicate that the Department had purchased access to Babel X between March 2022 and March 2023; it is unclear whether such access has continued.[48] In addition, the State Department's Global Engagement Center, which seeks to counter foreign disinformation and propaganda including by "violent extremist organizations," has disclosed that it uses a sentiment analysis tool known as SentiBERTIQ that was trained on "2.2 million labeled tweets spanning English, Spanish, Arabic, and traditional and simplified Chinese."[49] It is unclear whether the Department's Bureau of Intelligence and Research, which is a member of the Intelligence Community and therefore exempt from reporting AI use cases under federal law, uses Babel X, SentiBERTIQ, or equivalent tools.

Social media monitoring has typically demonstrated little in the way of effectiveness. In 2020, the Office of Information and Regulatory Affairs (OIRA) rejected a DHS proposal to expand its collection of social media identifiers on travel and immigration forms, ruling that it had not "adequately demonstrated the practical utility of collecting this information."[50] The following year, the Office of the Director of National Intelligence found that DHS's use of social media monitoring "resulted in very little impact" on the accuracy

---

[45] Cox, *Homeland Security Uses AI Tool*; and DHS, *Privacy Threshold Analysis (PTA)* (here).

[46] DHS, *Privacy Impact Assessment for Immigration and Customs Enforcement Operational Use of Publicly Available Information Including Social Media Information for Law Enforcement Investigations* (Dec.15, 2023) (here); Rachel Levinson-Waldman, Harsha Panduranga, and Faiza Patel, *Social Media Monitoring by the U.S. Government,* Brennan Center for Justice (Jan. 7, 2022) (here).

[47] *See* USASpending, *DHS Contract to Cobwebs America Inc*, PIID 70RDAD20C00000016 (visited July 1, 2024) (here). Additionally, the Office of Intelligence & Analysis (I&A) monitors social media to, among other asserted aims, counter "threats to homeland security." Spencer Reynolds and Faiza Patel, *A New Vision for Domestic Intelligence*, Brennan Center for Justice (Mar. 30, 2023) (here); I&A is known to target Americans' political views and speech, and it has done so to monitor people talking about abortion politics online, journalists, racial justice protestors, environmental activists, and others. *Id.*; *see also* Jana Winter, *DHS Monitored 'Social Media Reactions to Roe, Collected Legally Protected Speech, Bulletin Shows*, Yahoo!News (Nov. 16, 2022) (here); Shane Harris, *DHS Compiled 'Intelligence Reports' on Journalists who Published Leaked Documents*, Washington Post (July 30, 2020) (here); Alleen Brown, *Federal Agencies Pushed Extreme View of Cop City Protesters, Records Show*, Guardian (Dec. 6, 2023) (here). While I&A conducts some of this monitoring in-house, it also relies on purchased intelligence from a company that itself does social media monitoring, SITE Intelligence Group. *See* Ken Wainstein, *Under Secretary for Intelligence and Analysis Ken Wainstein Delivers Remarks at the Brookings Institution*, DHS (Sept. 21, 2023) (here); *Justification and Approval for Other Than Full and Open Competition, FY21-00280 (RIIA-21-00107)* (here). The SITE procurement documents do not require the company to be open with the government about its methods, undermining transparency and accountability.

[48] *See* Cox, *Homeland Security Uses AI Tool*; USASpending, *Department of State (DOS) Contract to Distributed Technology Group LLC*, PIID 19AQMM22F1250 (visited July 1, 2024) (here).

[49] Department of State, *AI Inventory* (visited July 1, 2024) (here).

[50] Office of Information and Regulatory Affairs, *View Generic ICR - OIRA Conclusion,* OMB (visited July 1, 2024) (here).

of screening visa applicants for possible terrorists.[51] Augmenting these practices with AI amplifies concerns about their accuracy and bias.

Sentiment analysis and some forms of predictive analytics derive from a subfield of AI and linguistics known as Natural Language Processing (NLP), which aims to build computer systems that interpret and manipulate human language.[52] NLP applications have typically struggled to accurately interpret linguistic nuances such as irony, satire, humor, and slang.[53] They also perform poorly on highly subjective and contextually specific tasks, such as identifying "extremist" content.[54] These inaccuracies all too frequently reflect harmful biases, such as a tendency to associate identity terms representing protected characteristics (such as "gay," "Black," or "Muslim") with anger and other negative sentiments.[55]

The turn towards building Large Language Models (LLMs)—which are trained on vastly more data and to perform a wide range of language-related tasks—complicates efforts to address these harms. In 2021, Stanford University researchers found that an older version of a popular LLM developed by OpenAI disproportionately associated Muslims with terrorism and violence.[56] A March 2024 study of five popular LLMs found that existing methods for mitigating racist bias entrench coded forms of racism, such as associating speakers of African-American English with unemployment and criminality.[57] The accuracy of LLMs further degrades when tasked with interpreting non-Latin derived languages that are poorly reflected in web data (the most common source of training data), such as Arabic and Urdu.[58]

These inaccuracies and biases exacerbate social media monitoring's existing harm to constitutional rights. Both of our organizations have documented how social media monitoring can mistakenly attribute criminal and threatening behavior to individuals, leading to wrongful arrests, interrogations, investigations, and refusal of entry at the border.[59] In 2020, for example, police in Wichita, Kansas, arrested a teenager on suspicion of incitement to rioting after he shared a threatening Snapchat screenshot to warn people

---

[51] *See* Charlie Savage, *Visa Applicants' Social Media Data Doesn't Help Screen for Terrorism, Documents Show*, New York Times (Oct. 5, 2023) (here).

[52] *See* Amazon Web Services, *What is Natural Language Processing (NLP)?* (visited July 1, 2024) (here).

[53] *See generally* Center for Democracy & Technology (CDT), *Mixed Messages? The Limits of Automated Social Media Content Analysis* (Nov. 2017) (here); Eleanor Shearer et al., *Racial Bias in Natural Language Processing*, Oxford Insights (Aug. 2019) (here).

[54] CDT, *Mixed Messages* at 16–17.

[55] *See* Anna Woorim Chung, *How Automated Tools Discriminate Against Black Language,* Civic Media (Jan. 24, 2019) (here); Shearer et al., *Racial Bias;* and Andrew Myers, *Rooting Out Anti-Muslim Bias in Popular Language Model GPT-3*, Stanford University Human-Centered Artificial Intelligence (July 22, 2021) (here).

[56] Andrew Myers, *Rooting Out Anti-Muslim Bias*.

[57] Valentin Hofmann et al., *Dialect Prejudice Predicts AI Decisions About People's Character, Employability, and Criminality* (Mar. 1, 2024) (here).

[58] Gabriel Nicholas and Aliya Bhatia, *Lost in Translation: Large Language Models in Non-English Content Analysis,* CDT at 17 (May 2023) (here).

[59] Levinson-Waldman, Panduranga, and Patel, *Social Media Surveillance by the U.S. Government;* Shaiba Rather and Layla Al, *Is the Government Tracking Your Social Media Activity?*, ACLU (Apr. 24, 2023) (here).

about potential violence.[60] This is the kind of contextual information that NLP tools can easily overlook.

AI may also introduce more noise, complexity, and error in social media monitoring operations that are already of questionable utility. Broad-scale monitoring of social media to detect threats and risks in the absence of any suspicion of wrongdoing has generated reams of useless information that crowd out real national security or public safety concerns.[61] In 2021, the former acting chief of DHS's Office of Intelligence and Analysis (I&A) admitted that real threats of violence on social media are "difficult to discern" from constitutionally protected speech, since they are frequently veiled in "vague inuendo" to evade platforms' content moderation systems.[62] It is doubtful that sentiment analysis and predictive analytics—which rely on the same NLP technologies used by these systems to parse social media content—will be more adept at identifying inuendo, or making constitutionally significant decisions about which online expression the government should investigate.

The questionable (to say the least) efficacy of social media monitoring, and its well-documented harms to civil liberties and rights, should lead PCLOB to examine whether introducing AI techniques has led to meaningful gains in the accuracy and utility of this practice. In particular, it should solicit case studies from agencies to test their claims about the usefulness of AI-facilitated social media monitoring in the vetting and screening of immigrants and travelers and the broad-scale detection of threats to combat terrorism. In analyzing these case studies, PCLOB should examine whether agencies have implemented adequate safeguards to protect privacy and civil rights and liberties, and whether non-AI strategies are better suited to facilitating the agency's investigation or identification of genuine security threats. If the agency is unable to produce case studies, or if PCLOB finds little evidence that social media monitoring has been effective, PCLOB should recommend that the agency cease this monitoring.

2. Use of AI to Screen Travelers and Immigrants

2.1 Risk assessments of people seeking to enter, leave, or travel within the United States.

PCLOB should examine the use of AI by CBP and TSA to screen and vet people traveling to, from, or within the United States. CBP today uses machine learning to conduct risk assessments of travelers at U.S. ports of entry.[63] In producing port-of-entry risk assessments, CBP applies machine learning to its "data holdings," which include

---

[60] *See* Rachel Levinson-Waldman and Angel Diaz, *How to Reform Police Monitoring of Social Media*, Brookings (July 9, 2020) (here); Amy Renee Leiker, *Outcry Follows Arrest of 2 Men Over Social Media Post that Urged Violence in Wichita Area*, The Wichita Eagle (June 8, 2020) (here).

[61] Levinson-Waldman, Panduranga, and Patel, *Social Media Surveillance by the U.S. Government*; Rather and Al, *Is the Government Tracking Your Social Media Activity*.

[62] DHS, *Examining the January 6 Attack on the U.S. Capitol: Testimony of Melissa Smislova* at 3 (Mar. 3, 2021) (here).

[63] DHS, *Artificial Use Case Inventory—Customs and Border Protection*: *Port of Entry Risk Assessments* (visited July 1, 2024) (here). In 2021, CBP stated that it used "predictive analytics," a type of analysis typically based on machine learning, as part of ATS's UPAX module, which generates risk assessments of travelers. *See* DHS, *2020 and 2021 Data Mining Report* (Aug. 2022) at 16 (here) [hereinafter Data Mining Report].

information amassed within DHS's Automated Targeting System (ATS).[64] ATS ingests huge volumes of information from dozens of databases from federal, state, and local governments, as well as from private brokers.[65] CBP runs an ATS "module" that "applies risk-based rules based on CBP officer expertise, analysis of trends of suspicious activity, and raw intelligence from DHS and other government agencies to assist CBP officers in identifying individuals who require additional inspection or in determining whether individuals should be allowed or denied entry into the United States."[66]

TSA also relies on ATS and related databases to conduct its own rules-based risk assessments through at least two programs: Silent Partner (international flights) and Quiet Skies (domestic flights).[67] Like CBP, TSA creates rules and runs them through ATS; passengers flagged under the rules may be subject to more intrusive screening.[68] CBP and TSA's risk-based screening programs are closely coordinated and mutually reinforcing; any use of AI by CBP almost certainly feeds into TSA's programs, and vice versa.[69] Through both CBP and TSA's programs, AI-driven risk assessments affect those traveling both internationally and domestically.

The public knows almost nothing about the AI systems CBP and TSA use to conduct these rules-based risk assessments, including how the agencies select and train the model(s) they rely upon, how the agencies monitor the systems' performance, and what measures the agencies have taken to ensure that their use of such systems is consistent with civil rights and liberties.

Any machine learning model trained on, or tasked with interpreting, data housed in or generated by ATS and related databases likely replicates and exacerbates the preexisting flaws in such datasets.[70] Although it has not been publicly confirmed, TSA and CBP likely

---

[64] DHS, *Artificial Use Case Inventory—Customs and Border Protection*: *Port of Entry Risk Assessments* (visited July 1, 2024) (here); Data Mining Report at 26.

[65] Data Mining Report at 21–22; DHS, *Privacy Impact Assessment Update for the Automated Targeting System*, DHS/CBP/PIA-006(e) at 2–3 (Jan. 13, 2017) (here) [hereinafter ATS Privacy Impact Assessment].

[66] Data Mining Report at 26; GAO, *Border Security: CBP Aims to Prevent High-Risk Travelers from Boarding U.S.-Bound Flights, But Needs to Evaluate Program Performance* (GAO-17-216) at 10 (Jan. 2017) (here) [hereinafter CBP GAO Report] ("CBP identifies unknown high-risk individuals by comparing their information against a set of targeting rules based on intelligence, law enforcement, and other information.").

[67] Data Mining Report at 29; DHS, *Privacy Impact Assessment Update for Secure Flight: Silent Partner and Quiet Skies*, DHS/TSA/PIA-018(i) at 1–2 (Apr. 19, 2019) (here) [hereinafter Secure Flight Privacy Impact Assessment].

[68] DHS, Office of Inspector General, *TSA Needs to Improve Management of the Quiet Skies Program* (OIG-21-11) at 1, 1 n.2 (Nov. 25, 2020) (here) [hereinafter DHS OIG Report].

[69] CBP GAO Report at 13; Data Mining Report at 28, 30; ATS Privacy Impact Assessment at 33–34; Secure Flight Privacy Impact Assessment at 7, 9, 34; GAO, *Aviation Security: TSA Coordinates with Stakeholders on Changes to Screening Rules But Could Clarify Its Review Processes and Better Measure Effectiveness* (GAO-20-72) at 7 (Nov. 2019) (here).

[70] As the ACLU explained in December 2023, at the U.S. Senate AI Insight Forum, "ATS and its associated systems run afoul of virtually every pillar for safe, effective, equitable, transparent, and fair algorithmic systems, including the principles laid out in the White House's Blueprint for an AI Bill of Rights." *U.S. Senate AI Insight Forum: National Security* (Dec. 6, 2023) (statement of Patrick Toomey, Deputy Director, National Security Project, ACLU) (here).

use the Terrorism Screening Dataset (TSDS or master watchlist),[71] one of the datasets included in ATS,[72] to train and build the machine learning models that generate and evaluate the rules-based risk assessment programs.[73] The TSDS reflects long-entrenched biases predominantly against American Muslims and those of Arab, Middle Eastern, or South Asian descent. A rough approximation of disproportionate impact is clear from the government's acknowledgment that as of February 2024, over one-third of watchlisted people are named Mohammed, Ahmed, Mahmoud, Abed, or Abdullah, or some spelling permutation of those common male Muslim names.[74] The TSDS is also riddled with error.[75] The bar for placement on the watchlist is extraordinarily low—in essence, suspicion that a person might be suspicious—and individuals innocent of any wrongdoing may be watchlisted, often without a meaningful process to challenge their placement.[76] Because AI systems amplify the biases and errors embedded in the datasets used to train those systems, it is likely that AI further entrenches the existing disparities in CBP and TSA's rules-based risk assessment programs.

The public also has almost no information about the use of AI to nominate individuals to the master watchlist and maintain them on it. The Threat Screening Center (TSC), an interagency body administered by the FBI and the hub of this system, has accepted nearly every nomination to the list put forward by agencies.[77] The low evidentiary standard for placement on the TSDS means that there are few safeguards against the TSC

---

[71] The TSDS was formerly known as the Terrorism Screening Database. Decl. of Samuel P. Robinson, *Khalid v. Gardland*, No. 21-cv-2307, ECF No. 19-1 at ¶ 5 (D.D.C. July 13, 2022).

[72] ATS Privacy Impact Assessment at 2–3.

[73] Some of the TSA rules at the heart of its rules-based risk assessment programs "are based on current terrorist travel trends, methods, techniques, or associations with Known or Suspected Terrorists on Federal Government watchlists," like the TSDS. DHS OIG Report at 1. The TSDS is also used to evaluate TSA's risk assessment programs. To measure success, TSA compares whether passengers flagged under a rules-based screening program are subsequently added to the TSDS. Data Mining Report at 30; DHS OIG Report at 20 (DHS response). CBP, for its part, uses its rules-based screening program to identify hundreds of "high-risk individuals" for inclusion in the TSDS. CBP GAO Report at 22. CBP also uses the information collected as part of its risk assessment programs "for future targeting efforts." *Id.* at 23.

[74] *See* Decl. of Steven L. McQueen, *Jardaneh v. Garland*, No. 18-cv-2415 (D. Md. Mar. 5, 2024) (on file with authors) (describing recent watchlisting data). According to a Council of American Islamic Relations analysis of a 2019 version of the watchlist, Muslim names comprise over 98% of the total entries. Council on American-Islamic Relations, *Twenty Years Too Many: A Call to Stop the FBI's Secret Watchlist* at 2 (2023) (here).

[75] *See Overdue Scrutiny* at 3 (describing the errors). The error rate is also apparent from the large number of U.S. persons removed from the No Fly List, a subset of the TSDS, as a result of litigation. *See* Brief for Amici Curiae at 14, *FBI v. Fikre*, 601 U.S. 234 (2024) (No. 22-1178) (here) [hereinafter *Fikre* Amicus Brief] (finding that 70 percent of U.S. persons who filed legal challenges to their placement on the No Fly List were removed during litigation).

[76] *Overdue Scrutiny* at 2–5; *Fikre* Amicus Brief at 4–11.

[77] The Threat Screening Center was formerly known as the Terrorist Screening Center. Decl. of Jason V. Herring, *Salloum v. Kable*, No. 19-cv-13505, ECF No. 37-1, ¶ 1 n.1 (E.D. Mich. June 21, 2021). For individuals with a purported nexus to international terrorism, agencies send nominations to the National Counterterrorism Center (NCTC), which maintains the derogatory information in the Terrorist Identities Datamart Environment (TIDE). And for individuals allegedly connected to domestic terrorism, nominations are managed by the FBI. *Overview of the U.S. Government's Watchlisting Process and Procedures* (Sept. 2020), *Khalid v. Garland*, No. 21-cv-2307, ECF No. 8-1 (D.D.C. Nov. 17, 2021); *Overdue Scrutiny* at 2.

relying on information that has been labeled "derogatory" by AI but may not have been closely reviewed or confirmed by human analysts.[78] Agencies are required to annually review their nominations of Americans to the TSDS, while TSC is required to conduct biannual reviews, but details about the depth or scope of these reviews are not publicly available.[79] And the lack of a meaningful redress process—the vast majority of people placed on the TSDS do not even receive official confirmation of their placement on it—means that individuals are unable to challenge their placement.[80]

There may be a dangerous feedback loop at play as well. CBP has confirmed that it has used its rules-based risk assessment programs in the past to identify individuals for nomination to the TSDS.[81] In other words, CBP may be relying on machine learning based on the biased and error-ridden data in the TSDS to identify individuals for rules-based risk assessments. It could then nominate persons identified through its risk assessment programs to the TSDS, which it, in turn, relies on to develop and refine the rules used in its risk assessment programs. This circular process may easily perpetuate and exacerbate the existing bias and errors in both the TSDS and rules-based screening.

Public information about the AI systems used by CBP and TSA to conduct rules-based risk assessments and by other federal agencies to nominate and/or place people on the watchlist is especially important given the dangers that such technologies can pose for people's civil rights and civil liberties. Much as in areas like law enforcement, using algorithmic systems to amass and analyze information, classify individuals as potential "threats," and make decisions about who should be questioned or searched, can perpetuate discrimination, intrude on privacy, and lead to wrongful denials of entry. Records from the master watchlist are widely disseminated to thousands of state, local, and tribal law enforcement agencies nationwide, as well as approximately 60 foreign countries.[82] Built-in bias and flawed algorithms may therefore lead to additional or wrongful investigation of individuals, exposing them to prolonged questioning, intrusive searches, or even detention at ports of entry both in the United States and abroad.

Little is known about the efficacy of CBP's and TSA's AI tools, or what safeguards for civil rights and civil liberties are in place. PCLOB should use its independent oversight authority to educate the public about how the agencies' rules-based risk assessment programs work generally and provide additional information about biases, error rates, and other flaws in the datasets underlying CBP and TSA's use of AI and rules-based risk assessments. PCLOB should evaluate whether CBP and TSA's use of AI accounts for such problems and what steps the agencies have taken to address such urgent concerns. And were PCLOB to find that CBP and TSA's guardrails against faulty data, unproven AI, or

[78] *Overdue Scrutiny* at 2–5; *Fikre* Amicus Brief at 4–11.

[79] *Overdue Scrutiny* at 2.

[80] *Id.*

[81] CBP GAO Report at 22–23. As of 2019, TSA did not nominate individuals matching Silent Partner or Quiet Skies rules to the TSDS unless they were "involved in a security incident that would support such nomination." Secure Flight Privacy Impact Assessment at 3.

[82] Decl. of Timothy P. Groh, *Elhady v. Piehota*, No. 16-cv-375, ECF No. 308-24 (E.D. Va. Mar. 12, 2019).

discriminatory decision-making are insufficient—or non-existent—PCLOB should call on CBP and TSA to suspend their rules-based risk assessment programs entirely.

2.2 Review and adjudication of applications for immigration benefits.

PCLOB should also closely examine any use of AI to review or adjudicate applications for immigration benefits, including applications to adjust status or naturalize. U.S. Citizenship and Immigration Services (USCIS), the agency responsible for reviewing, granting, and denying applications for immigration benefits, has stated it that it "may" integrate AI into its processes for determining whether applicants for immigration benefits "pose a threat to national security."[83] Specifically, USCIS's Fraud Detection and National Security Directorate (FDNS), which is tasked with "ensur[ing] that immigration benefits are not granted to individuals who may pose a threat to national security and/or public safety," indicates that it "may use [AI] data" to "aid in investigative work, enhance investigative case prioritization, and detect duplicate case work."[84]

These vague statements sound alarm bells. USCIS has long relied on flawed and discriminatory criteria to baselessly label applicants for immigration benefits as "national security concerns." Indeed, since at least 2008, under a policy known as the Controlled Application Review and Resolution Program (CARRP), USCIS has branded tens of thousands of applicants for immigration benefits as "national security concerns," which can be based on immigration officers' subjective impressions of applicants' personal history and affiliations.[85] According to USCIS, innocuous characteristics shared by millions of people—*e.g.*, knowledge of a second language, advanced education, religious activity, or travel through wide areas of the globe—are enough for an applicant for immigration benefits to be deemed a "national security concern."[86] USCIS expressly instructs its officers to err on the side of labeling applicants for immigration benefits as "national security concerns," even when law enforcement agencies disagree.[87]

There is no evidence that USCIS's longstanding processes for labeling applicants for immigration benefits as "national security concerns" are valid or reliable. By contrast, there is extensive evidence that those same processes disparately impact people who are Muslim or perceived to be Muslim. For instance, an expert analysis of USCIS data from fiscal years 2012–2019 has demonstrated that USCIS labeled applicants for immigration benefits from Muslim-majority countries as "national security concerns" at more than 10 times the rate of

---

[83] DHS, *Artificial Use Case Inventory—U.S. Citizenship and Immigration Services*: *FDNS-NextGen* (visited July 1, 2024) (here).

[84] *Id.*

[85] A forthcoming briefing paper by the ACLU and its partners describes CARRP in greater detail. For additional information, see Jennie Pasquarella, *Muslims Need Not Apply* at 2–5, ACLU of Southern California (Aug. 21, 2013) (here).

[86] Attachment A - Guidance for Identifying National Security Concerns at 3–4, *Wagafe v. Biden*, No. 17-cv-94, ECF No. 645-54 (W.D. Wa. Nov. 17, 2023) (here); *see also* International Refugee Assistance Project, *Debunking "Extreme Vetting": Recommendations to Build Back the U.S. Refugee Admissions Program* at 16 (June 2021) (here) (describing application of CARRP in context of U.S. Refugee Admissions Program).

[87] Exhibit 36 to Pasquarella Decl. at 58, *Wagafe v. Biden*, No. 17-cv-94, ECF No. 645-55 (W.D. Wa. Nov. 17, 2023) (here).

applicants from non-Muslim-majority countries.[88] The effects of such labeling are dire: when USCIS deems someone a "national security concern," the agency takes more than twice as long to adjudicate their application for immigration benefits, and it is at least twice as likely to deny the application—even when it ultimately concludes that the person does not, after all, fit within the agency's expansive definition of "national security concern."[89]

Integrating an AI system or model into the process of reviewing and adjudicating applications for immigration benefits risks replicating (or exacerbating) the agency's existing, deeply flawed processes for identifying "national security concerns"—with corresponding impacts on applicants' rights to due process and equal protection.[90] To that end, PCLOB should exercise its independent oversight authority to provide the public with information about precisely how USCIS selects, trains, and assesses the performance of any AI system or model that it uses in the review or adjudication of applications for immigration benefits.

3. Use of AI for Facial Recognition

As our organizations have explained in other contexts,[91] the use of facial recognition technology (FRT) poses several serious threats to civil liberties and civil rights, making it dangerous both when it fails and when it functions.[92] The Board should examine the use of FRT in the government's various counterterrorism activities, including those that intersect with law enforcement and immigration.[93]

FRT is unreliable and biased. Even under optimal conditions, FRT systems are not designed to provide positive identification. Rather, at most, the technology provides an

---

[88] Suppl. Expert Report of Sean M. Kruskol ¶ 9, *Wagafe v. Biden*, No. 17-cv-94, ECF No. 645-14 (W.D. Wa. Nov. 17, 2023) (here).

[89] Pls.' Br. at 5, *Wagafe v. Biden*, No. 17-cv-94, ECF No. 634 (W.D. Wa. Oct. 30, 2023) (here); Ex. AV to Suppl. Expert Report of Sean M. Kruskol, *Wagafe v. Biden*, No. 17-cv-94, ECF No. 645-14 (W.D. Wa. Nov. 17, 2023) (here).

[90] Underscoring these risks, USCIS trains immigration officers to use information contained in or generated by ATS to label applicants for immigration benefits as "national security concerns." Identifying and Documenting NS Concerns at 44, *Wagafe v. Biden*, No. 17-cv-00094, ECF No. 666-19 (June 13, 2024) (here).

[91] ACLU, *Re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Executive Order 14074, Section 13(e))*, (Jan. 19, 2024) (here). ACLU, *Response to U.S. Commission on Civil Rights Request for Comment on Civil Rights Implications of the Federal Use of Facial Recognition Technology* (April 8, 2024) (here); Faiza Patel and Angel Diaz, *Face it: This Is Risky Tech,* Brennan Center for Justice (Aug. 16, 2018) (here); Brennan Center for Justice, *Coalition Statement Highlights Major Civil Rights Concerns with Face Recognition* (June 3, 2021) (here).

[92] In recognition of these dangers, more than 20 jurisdictions—including Boston; Minneapolis; Pittsburgh; Jackson, Mississippi; San Francisco; King County, Washington; and the State of Vermont—have enacted legislation halting most or all law enforcement or government use of face recognition technology. Others, such as the states of Maine and Montana, have enacted significant restrictions on law enforcement use of the technology. And law enforcement agencies in jurisdictions such as New Jersey and Los Angeles have prohibited use of Clearview AI, an FRT vendor that markets a particularly privacy-destroying system built on a database of tens of billions of non-consensually collected faceprints.

[93] The ACLU has repeatedly called for a federal moratorium on the use of facial recognition by law and immigration enforcement agencies. *See, e.g.*, Press Release, ACLU, ACLU Calls for Moratorium on Law and Immigration Enforcement Use of Facial Recognition (Oct. 24, 2018) (here).

"algorithmic best guess."[94] It will frequently produce possible matches that are incorrect.[95] The accuracy of the technology is affected by several factors, including the performance and training of the algorithm, the makeup of the matching database, and the features of the probe image (including angle, lighting, occlusion, and pixelation).[96] Most disturbingly, the technology continues to have markedly higher false match rates for people of color and women than for white people and men.[97]

Proposals to mitigate these harms often recommend using FRT algorithms with relatively higher accuracy rates and relatively lower demographic disparities. Although well-intentioned, these proposals rest on unstable ground. Current FRT accuracy tests do not reflect the conditions of real-world FRT use.[98] Additionally, testing data is difficult to interpret, is susceptible to manipulation, and is difficult to compare across algorithms.[99]

Despite these flaws, government use of FRT continues to expand rapidly. Most publicly disclosed uses involve trying to identify suspects or confirm individuals' identities based on photographs or from still frames extracted from video. However, the use of video face recognition surveillance looms—raising the threat of pervasive, suspicionless surveillance—as national and homeland security agencies widely experiment with and deploy AI-powered facial recognition tools.[100] For instance:

NSA and DOD. As far back as 2014, it was reported that the NSA was collecting millions of images of people from communications it collects through its surveillance programs.[101] Very little information about the NSA's use of its vast database of images has been made public. But in a 2019 presentation obtained by the ACLU through FOIA litigation, the Intelligence Advanced Research Project Agency described a program called "Janus" whose goal was to "dramatically improve face recognition performance in massive

---

[94] Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, The New Yorker (Nov. 13, 2023) (here); *see also* Nat'l Acad. of Sci., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* at 48–49 (2024) (here).

[95] Because FRT systems conducting one-to-many searches are generally configured to produce multiple possible matches, even when the algorithm identifies a true match, it will also necessarily generate numerous false matches.

[96] Nat'l Acad. of Sci., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* at 47 (2024) (here).

[97] *Id.* at 24, 56–57.

[98] Clare Garvie, *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations* at 15–16, Geo. L. Ctr. on Privacy & Tech. (Dec. 6 2022) (here).

[99] Marissa Gerchick and Matt Cagle, *When it Comes to Facial Recognition Technology, There Is No Such Thing as a Magic Number*, ACLU (Feb. 7, 2024) (here); *Facial Recognition: Current Capabilities, Future Prospects, and Governance* at 46 (2024) (here).

[100] *See, e.g.*, ACLU, Comment re: DHS Information Collection Request (Dec. 6, 2021) (here); *see also* GAO, *Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections* (GAO-22-106100) (June 29, 2022) (here) (indicating that DOD, DHS, DOJ, and DOS had reported using facial recognition technology for national security and defense related purposes). Section 5708 of the FY2020 National Defense Authorization Act mandated that the Director of National Intelligence submit a report on the use of facial recognition technology. This report has never been made public despite it being required to have been submitted in an unclassified form.

[101] James Risen and Lauren Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. Times (May 31, 2014) (here).

video collections."[102] Janus aimed to enable facial recognition surveillance of "millions of subjects," including based on "partial, incomplete, and occluded views" of faces, and at "target distances" of more than a half-mile.[103] This capability was designed to tap footage from surveillance cameras and flying drones in public places, such as subway stations and street corners. This could pose serious risks to privacy and First Amendment protected activities if it is used to, for example, identify protestors for surveillance and other measures.

FBI. The FBI uses FRT for intelligence and national security purposes and has disclosed its use of these tools to search for persons associated with open assessments.[104] These assessments can be opened by agents without any suspicion of criminal activity so long as they have an "authorized purpose" such as preventing crime or terrorism.[105] A 2021 GAO Report also shows the "Janus" program is "in development" at the FBI and currently being used for research and education purposes.[106] It has also contracted with Clearview AI, a company that has scraped tens of billions of photos from the internet to extract biometric faceprints without consent.[107] The FBI has also worked with ICE to use FRT on state driver's license databases to search for suspects. Despite its expanding FRT capabilities and access to facial photos, the FBI has deployed the technology without adequate testing, training, and safeguards.[108]

TSA and CBP. TSA and CBP are both currently using facial recognition systems that could eventually be used on all domestic and international fliers.[109] The use of this technology by CBP and the TSA is especially concerning, given their history of tracking and spying on journalists,[110] subjecting travelers to excessive and humiliating searches,[111] and bias-based targeting and interrogation of people based on national origin, religious beliefs, or political views.[112] PCLOB should examine how these efforts are being integrated with

---

[102] Intelligence Advanced Research Projects Agency, *Janus: Radically Expanding the Scenarios in Which Automated Face Recognition Can Establish Identity* (here).

[103] Drew Harwell, *FBI, Pentagon Helped Research Facial Recognition for Street Cameras, Drones*, Wash. Post. (Mar. 7, 2023) (here).

[104] *House Oversight and Reform Committee: Facial Recognition Technology - Ensuring Transparency in Government Use* (June 4, 2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, FBI) (here); *U.S. Senate AI Insight Forum: National Security* (Dec. 6, 2023) (statement of Patrick Toomey, Deputy Director, National Security Project, ACLU) (here).

[105] Michael German and Kaylana Mueller-Hsia, *Focusing the FBI*, Brennan Center for Justice (July 28, 2022) (here).

[106] Harwell, *FBI, Pentagon Helped Research Facial Recognition for Street Cameras, Drones.*

[107] *Id.*

[108] GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (GAO-21-518) (June 3, 2021) (here).

[109] *See* Jay Stanley, *TSA Testing Face Recognition at Security Entrances, Opening Door to Massive Expansion of the Technology*, ACLU (Aug. 29, 2019) (here).

[110] Scarlet Kim, Esha Bhandari, and Mitra Ebadolahi, *The U.S. Government Tracked. Detained, and Interrogated Journalists. We're Suing on Their Behalf.*, ACLU (Nov. 20, 2019) (here).

[111] Hugh Handeyside, *The Watchlisting System Exemplifies the Government's Post-9/11 Embrace of Biased Profiling*, ACLU (Sept. 9, 2021) (here).

[112] Scarlet Kim and Hugh Handeyside, *CBP Lied About Iranian-American Detentions, Leaked Memo Suggests*, ACLU (Feb. 3, 2020) (here).

other parts of DHS and other intelligence agencies, particularly any efforts to use this system to run faces against criminal, intelligence, or immigration watchlists.

We urge PCLOB to examine and report on the following:

FRT use cases. The Board should examine how agencies like the NSA, CIA, and National Counterterrorism Center (NCTC) use FRT and whether they are collecting facial imagery of people in the United States from social media or through the purchase of commercially available information.

FRT false positives and their consequences. The Board should examine whether the national and homeland security agencies have policies in place that measure false positive rates and report on the consequences of any misidentified matches by these agencies, such as generating misleading or otherwise inaccurate intelligence on security threats, intrusive surveillance or investigation, wrongful detentions or questioning at the border, wrongful denial or revocation of immigration benefits, or unjustified security clearance denial or revocation, which can impact a person's federal or other employment.

FRT aggregate data. The Board should report aggregate data on FRT use across national and homeland security agencies affecting people in the United States—including, by agency:

> (1) aggregate information on the use of FRT, including: (A) the total number of facial recognition searches; (B) the total number of searches for counterterrorism and intelligence gathering purposes, catalogued by their specified purpose; (C) the total number of searches that have been performed on facial images collected in public places; (D) the percentage of searches that identified people in the United States, whether intentionally or incidentally; (E) the total number of searches that generated leads; and (F) demographic breakdown of individuals in probe photos by race and sex;
>
> (2) information about the FRT system and algorithm(s) used, including vendor, version, and similarity threshold; and
>
> (3) a log of facial recognition searches, including (A) the requesting agency or field office; (B) the purpose of the search; (C) the race and sex of individual in the probe photograph; (D) whether the search generated results; (E) whether a facial recognition lead was provided to the requesting agency, field office, or officer; and (F) whether any individual appearing as a possible match in the FRT search was subsequently investigated, questioned, or searched; denied an immigration, travel, or employment benefit; or arrested or charged (depending on the agency).

4. Use of AI to Identify or Recommend Targets for Lethal Strikes

The Department of Defense is racing to develop and deploy AI in one of the government's most dangerous activities: lethal counterterrorism operations abroad. While the U.S. military's investment in AI is enormous and wide-ranging, recent reporting on DOD's flagship AI effort, Project Maven, indicates that this includes the operational use of

AI tools to identify or recommend targets for lethal strikes.[113] Yet the public still knows very little about these systems and what safeguards, if any, are in place to ensure lawfulness, accuracy, and minimize harm to civilians.[114]

According to media reports in recent months, the U.S. military is actively deploying the Maven Smart System—an AI-powered system under Project Maven that trains itself to recognize personnel and equipment and to identify environmental changes that correspond to new permissible targets, like military facilities.[115] In addition to video imagery, Maven Smart System relies on data from radar systems, heat-detecting infrared sensors, and nonvisual information, like geolocation tags from social media accounts and electronic surveillance.[116] DOD has used this system and other AI-powered systems under Project Maven in combat operations, claiming that it "located rocket launchers in Yemen and surface vessels in the Red Sea, and helped narrow targets for strikes in Iraq and Syria," including rockets, missile storage, drone facilities, and militia operation centers.[117] As one U.S. colonel leading these AI targeting efforts put it, Project Maven "showed [him] the art of the possible."[118]

The shift to AI-based target identification could vastly increase the speed and scale of military targeting decisions, and thereby magnify the destructive impact of errors. By some estimates, AI-assisted targeting could allow a commander to approve up to 80 targets an hour, as opposed to 30 targets without the system.[119] While AI systems like Project Maven may greatly increase the speed at which potential targets can be nominated, their use in real-world conditions raises serious concerns. For example, while human analysts correctly identify objects about 84 percent of the time, the Maven system does so only 60 percent of the time; and accurate identification can even plummet below 30 percent when conditions such as snow make images less clear.[120] Virtually nothing is known about the reliability of the imagery datasets used to train and test this system. Meanwhile, other AI-based targeting systems may also rely on various types of data—including cell phone location data and communications metadata—to nominate potential human targets with questionable accuracy—or legality.[121]

---

[113] *See, e.g.*, Katrina Manson, *AI Warfare Is Already Here*, Bloomberg (Feb. 28, 2024) (here); Lori Ann LaRocco, *A Network of Sensors Is Helping U.S.-Led Forces Detect Threats in the Red Sea*, CNBC (Jan. 10, 2024) (here).

[114] The ACLU and the Brennan Center understand that the PCLOB is limited by statute in its ability to seek access to information about covert actions from U.S. government agencies, *see* 42 U.S.C § 2000ee(g)(5), but the AI-assisted lethal strikes described here do not fall within that limitation.

[115] Manson, *AI Warfare Is Already Here*.

[116] *Id.*

[117] *Id.*; Piero Cingari, *U.S. Military Utilizes AI In Middle East Operations: 'We've Been Using Computer Vision'*, Benzinga (Feb. 26, 2024) (here).

[118] Manson, *AI Warfare is Already Here.*

[119] *Id.*; *Cf.* Yuval Abraham, *'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza*, +972 Magazine (Apr. 3, 2024) (here) (reporting that human reviewers could approve "dozens" of strikes a day using Israel's Lavender AI system, spending as little as twenty seconds to confirm each of the AI-selected targets).

[120] Manson, *AI Warfare is Already Here.*

[121] *Cf.* Lee Ferran, *Ex-NSA Chief: 'We Kill People Based on Metadata'*, ABC News (May 12, 2014) (here); Abraham, *'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza*.

Similarly, little is known about what requirements or processes DOD has in place to ensure careful human review and lawful approval of AI-selected targets, especially given the significant error rates cited above. But even with a human "in the loop," the pressure to approve and keep pace with new targets generated by AI systems could result in only cursory human review and, at scale, enormous destruction. Reporting on other countries that have used similar AI targeting systems underscores this peril, revealing a world of warfare where "human agency and precision [are] substituted by mass target creation and lethality."[122]

As DOD expands its use of AI in counterterrorism operations, PCLOB should not only examine the ways in which AI is being deployed to direct lethal strikes, but also demand transparency about these systems' error rates, testing, and human review requirements. Even one errant strike can have devastating consequences for civilians. The risk of increasing automation is that the demand for ever-greater speed in target selection will lead to immense human tragedy and suffering. Should the Board find that these systems are unreliable in real-world contexts, have not been sufficiently tested, or lack robust safeguards, it should demand that the use of such AI tools be suspended before they cause tremendous harm.

5. Use of AI to Protect "Soft Targets" in the United States

As part of its stated mission to "[c]ounter terrorism and homeland security threats," DHS says that it is "promoting a dynamic process to assess soft targets and address security gaps, and investing in research and development for technological solutions."[123] DHS defines "soft targets" as crowded places such as sporting venues and shopping centers. While there may be a legitimate need to protect such venues, DHS has historically imported flawed counterterrorism methods to do this work, including baseless Suspicious Activity Reporting and behavioral indicator programs,[124] using electronic surveillance tools such as IMSI catchers without proper authorization,[125] discriminatory and unreliable screening and vetting of immigrants and travelers,[126] the isolation of protestors to remote designated zones,[127] and more.[128] Incorporating AI into these activities can only further implicate sensitive privacy and civil liberties issues that PCLOB should closely examine, like the use of AI in the generation and sharing of domestic intelligence, or the use of "technological solutions" to monitor and track people in public places.

---

[122] Abraham, *'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza* (describing the "Lavender" AI system that Israel uses to identify human targets).

[123] DHS, *Counter Terrorism and Homeland Security Threats* (last updated May 30, 2023) (here).

[124] Mike German, Rachel Levinson-Waldman, and Kaylana Mueller-Hsia, *Ending Fusion Center Abuses*, Brennan Center for Justice at 7 (Dec. 15, 2022) (here).

[125] Office of Inspector General, *Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators,* OIG-23-17, DHS (Feb. 23, 2023) (here); Matthew Guariglia, *Report: ICE and the Secret Service Conducted Illegal Surveillance of Cell Phones,* Electronic Frontier Foundation (Mar. 2, 2023) (here).

[126] *See* Section 2, Use of AI to Screen Travelers and Immigrants, of this submission.

[127] Lorin Cox, *What First Amendment Lawsuit Means for Designated Protest Zones at RNC in Milwaukee,* Wisconsin Public Radio (June 24, 2024) (here).

[128] Ed Pilkington, *'These Are His People': Inside the Elite Border Patrol Unit Trump Sent to Portland,* Guardian (July 27, 2020) (here).

One way DHS has pursued its goals is by funding an industry/academic research and development center called SENTRY (Soft Target Engineering to Neutralize the Threat Reality), which aims to create "resources and tools for anticipating and mitigating threats to soft targets and crowded places."[129] Among the center's research areas are "advanced sensing technologies," a field aimed at "developing new sensing capabilities to detect threats"—in particular, "to establish new stand-off sensor concepts for detecting concealed threats in crowds."[130] SENTRY research projects include AI tools "for data mining of social media, geospatial data platforms, and other sources of information to extract insights on potential threats," and AI for "risk assessment, quantitative threat deterrence, development of layered security architectures; and providing methods for fusing data and other information."[131]

Similarly, DHS's Silicon Valley Innovation Program, which funds private companies to research and develop products that DHS would like to see, has solicited applications aimed at "Securing Soft Targets."[132] Under this portfolio, it currently funds companies working to "build AI algorithms that link objects (e.g., unattended baggage) to people and track them," to "identify motion of interest from security video feeds," and to create an "anomaly detection system that leverages activity recognition and tracking to capture multiple data points per subject."[133] DHS has also been testing various sensors and detectors intended to be used in public spaces. For several years, the agency has been carrying out public tests of thermal cameras designed to spot weapons and explosives underneath people's clothing.[134] Various at-a-distance AI scanner technologies are also being researched by participants in the SENTRY program.[135]

Most of these efforts target people going about their business in public places, generally unaware of the AI technologies that are being trained upon them. Some, if not all—including those that use AI in surveillance and in attempts to measure "suspiciousness"—raise significant issues of privacy, chilling effects, discrimination, and other potential harms. The use of AI machine vision to monitor people, for example, even when done in an ostensibly anonymous manner, has the potential to significantly change the experience of being in public in the United States, as the ACLU detailed in its 2019 report on the subject.[136]

---

[129] SENTRY, *Overview* (visited July 1, 2024) (here).

[130] SENTRY, *Research* (visited July 1, 2024) (here).

[131] SENTRY, *Year 2 Annual Report for Narrative July 1, 2022 – June 30, 2023* (Aug. 31, 2023) at 15 (here).

[132] DHS, *Securing Soft Targets* (last updated Jan. 31, 2024) (here).

[133] *Id.*

[134] Rashida Richardson and Jay Stanley, *TSA Tests See-Through Scanners on Public in New York's Penn Station,* ACLU (Mar. 2, 2018) (here); Jay Stanley, *New Point-and-Shoot Chemical Detectors Raise Privacy and Constitutional Issues,* ACLU (Dec. 6, 2023) (here).

[135] Vito Levi D'Ancona, *Concealed Threat Detection From a Distance*, Mantacus (Nov. 15, 2023) (here); SENTRY, *ASDA27: Implementation and Deployment of Situational Awareness Strategies for Protecting Soft Targets* (visited July 1, 2024) (here); SENTRY, *Agenda for Tuesday, November 13, 2023 Day 1* (July 1, 2024) (here).

[136] Jay Stanley, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy*, ACLU (June 13, 2019) (here). Unlike many uses of AI that are likely developing within other agencies, the Department of Homeland

At its worst, AI-facilitated surveillance of public venues may lead to the harassment, investigation, and arrest of individuals and groups that are already disproportionately singled out for scrutiny, such as protestors, communities of color, and immigrants. These activities can also lead to the "airportization" of American life by encouraging local authorities to increase the use of security perimeters, searches, and surveillance at an ever-widening scope of public gatherings and events.[137] Such efforts may lock down American life in ways that impose not only direct costs (the price of equipment and personnel), but also inefficiencies (such as wait times and efforts to avoid false alarms by the public) and the intangible social and psychological costs that come from surveillance, submission to authority, and the lack of an open society. Given the sensitivity of using surveillance on people in public places, these activities warrant close scrutiny.

AI Safeguards and Recommendations

The little we know about the federal government's adoption of AI for counterterrorism and related national security purposes has surfaced serious risks to privacy, civil liberties, and civil rights. To prevent and mitigate these risks, PCLOB should:

Investigate the adequacy of safeguards. PCLOB should examine what, if any, safeguards agencies have implemented to protect privacy, civil liberties, and civil rights when they use AI in counterterrorism and related national security operations, and whether these comply with the forthcoming NSM. PCLOB should also examine how these safeguards differ from the minimum risk management practices established under OMB Memo M-24-10, and whether these discrepancies pose risks to privacy, civil liberties, and civil rights.

OMB's risk management practices include commonsense measures such as impact assessments (which examine whether the risks of deployment outweigh its benefits), real-world testing (to identify and mitigate any errors before a system goes live), public notice (to provide the public with accessible information about how agencies are using AI), and ongoing risk monitoring (to identify and address unanticipated risks). OMB Memo M-24-10 does not apply to AI used in national security systems, and specifically exempts DOD and members of the Intelligence Community from these practices. But OMB has encouraged intelligence agencies to follow these baseline standards, as they reflect best practice on mitigating AI's risks and harms.

If PCLOB finds that the NSM's safeguards are insufficient, it should urge the White House to require DOD, the Intelligence Community, and national security agencies to comply with OMB's minimum risk management practices. It should also recommend that Congress enact these practices without any carveouts for DOD, the IC, or national security systems.

Security as a domestic agency is typically more open about its projects. The management of SENTRY, for example, has invited the ACLU to participate in and present at several of their meetings, and DHS has been public about its SVIP awards and its testing of standoff weapons and chemical detectors. Nonetheless, there may be other activities underway that have not been made public, as well as important nonpublic details about those that have.

[137] DHS, *Software Suite Will Harden Defenses for Soft Targets* (Nov. 3, 2022) (here).

Critically examine the efficacy of AI-enabled operations. Many of the use cases discussed above have yielded questionable intelligence, are based on flawed and discriminatory technology, or are, at best, unproven. For each of these use cases, PCLOB should consider the efficacy and risks of the underlying programs, examining the extent to which reliance on AI is necessary to accomplishing the agency's counterterrorism or national security objective and whether non-AI strategies (particularly those that are less data-driven and biased) would have been equally or better suited to accomplishing this objective. It should develop and publish metrics for conducting this analysis, such as those that capture whether AI has mitigated or amplified inaccuracies and biases embedded in the underlying program. When agencies outsource the development and operation of AI systems to government contractors, PCLOB should examine whether agencies have independently evaluated the contractor's claims about the efficacy of the system (such as by conducting independent testing of the system pre-acquisition).[138]

Recommend restrictions. PCLOB should urge relevant agencies to cease any use of AI that it has determined is: (1) not sufficiently tested; (2) unreliable or otherwise ineffective; or (3) raises risks to privacy, civil liberties, civil rights, or safety that cannot be effectively mitigated. This would establish a minimum threshold for AI use in counterterrorism and national security operations that aligns with OMB Memo M-24-10's requirement that agencies suspend AI use if the "expected benefits of the AI functionality . . . do not meaningfully outweigh the risks."

Recommend stronger oversight. PCLOB should examine what steps Chief Artificial Intelligence Officers (CAIOs) are taking to ensure that national security systems comply with the NSM, and which OMB risk management practices they are implementing even if their agencies are not bound by them. It should also examine how rights-focused oversight mechanisms, such as the Department of Justice's Office of Privacy and Civil Liberties and DHS' Privacy Office, should be integrated into AI oversight protocols. Finally, PCLOB should review whether Inspector Generals' offices have sufficient capacity, resources, and expertise to audit and investigate fraud, waste, and abuse facilitated by AI use in the intelligence community and national security systems. These reviews should provide the basis for recommendations to Congress on how these offices should be staffed, resourced, and empowered to conduct effective oversight.

* * *

The ACLU and the Brennan Center appreciate the opportunity to provide input to the Board on this important topic. If you have any questions about these comments, please do not hesitate to contact: at the ACLU, National Security Project Deputy Director Patrick Toomey (ptoomey@aclu.org), and Senior Policy Counsel Kia Hamadanchy (KHamadanchy@aclu.org); and at the Brennan Center, Senior Director Faiza Patel (patelf@brennan.law.nyu.edu) and Senior Counsel Amos Toh (toha@brennan.law.nyu.edu).

---

[138] *See* Brennan Center for Justice and Electronic Privacy Information Center, *Comment Submitted to the Office of Management and Budget on Federal Procurement of Artificial Intelligence* (Apr. 29, 2024) (here).

Sincerely,

Patrick Toomey
Charlie Hogle
Hina Shamsi
ACLU National Security Project

Faiza Patel
Senior Director
Liberty and National Security Program

Kia Hamadanchy
Senior Policy Counsel
ACLU National Political Advocacy Dept.

Amos Toh
Senior Counsel
Liberty and National Security Program