Comments of Patrick G. Eddington
Senior Fellow, Cato Institute
Regarding Notice-PCLOB-2024-01, Docket No. 2024-0002, Sequence No. 24
for the
Privacy and Civil Liberties Oversight Board
June 21, 2024

To Whom It May Concern:

In response to the Board's May 23, 2024, *Federal Register* notice "PCLOB Public Forum Examining the Role of Artificial Intelligence in Counterterrorism and Request for Public Comment," I offer the following comments, suggestions, and questions. I note that these are my views offered in my capacity as a Senior Fellow at the Cato Institute and do not necessarily represent the views of the Institute, its management, or its board of directors.

In responding to the Board's request for comments, I've keyed my responses to several of the specific questions the Board itself raised in its *Federal Register* notice.

1. How is the federal government using AI in current efforts to combat terrorism and protect national security?

In the four years since then-President Trump issued Executive Order 13690 on AI use in the federal government, it's become clear that the current federal approach to setting across-the-board AI standards government-wide has failed.[1] A December 2023 Government Accountability Office (GAO) report revealed as much.[2] Indeed, six months before Trump issued that EO, his ODNI issued IC-wide guidance regarding AI standards and ethical conduct.[3] To the best of the author's knowledge, no specifics regarding exactly how the IC is employing AI in the counterterrorism (CT) context--whether targeting individuals or groups overseas or domestically--has been made public.

I have particular concerns with respect to how federal law enforcement agencies charged with a CT mission may already be employing AI.

In his June 4, 2024, testimony before the Senate Appropriations Committee's Subcommittee on Commerce, Justice, Science, and Related Agencies, FBI Director Chris Wray mention AI only

[1] Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Governm*ent, December 3, 2020.
[2] Government Accountability Office, *Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements*, GAO-24-105980, December 2023.
[3] Intelligence Community Releases Artificial Intelligence Principles and Framework. ODNI News Release No. 27-20, July 23, 2020. Available online at https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2020/3468-intelligence-community-releases-artificial-intelligence-principles-and-framework

once, in the context of "sextortion" schemes targeting children.[4] Absent from Wray's statement for the record was any indication of what measures, if any, the Bureau is taking to ensure its own agents are not employing AI tools in ways that potentially threaten the First and Fourth Amendment rights of U.S. Persons. In light of the FBI's many and well-documented abuses of the FISA Section 702 database, this concern is hardly a hypothetical one.

Moreover, EOs and department/agency guidance can change from administration to administration. This is why some type of Congressional action requiring scrupulous adherence by federal agencies and departments to the letter and the spirit of the First and Fourth Amendments in any employment of AI is absolutely critical.

2. How can or should AI be used for targeting, behavioral profiling, signals analysis, intelligence analysis, and prediction?

Twice in the last decade, the GAO has published reports declaring the Transportation Security Administration's (TSA's) aviation threat behavior detection indicators invalid and not scientifically based.[5] As GAO investigators noted in their November 2013 report on the TSA's Screening of Passengers by Observation Techniques (SPOT) program, "GAO reviewed four meta-analyses (reviews that analyze other studies and synthesize their findings) that included over 400 studies from the past 60 years and found that the human ability to accurately identify deceptive behavior based on behavioral indicators is the same as or slightly better than chance."[6]

In October 2016, *The Intercept* reported on a SECRET 2012 FBI survey of some 200 terrorism cases in which the Bureau found that "It can be difficult, if not impossible, to predict for any given individual what factor or combination of factors will prompt that individual's radicalization or mobilization to violence."[7]

These findings alone should convince an objective observer that trying to use AI for threat behavior detection at the individual person level would be a fool's errand bound to lead to constitutional rights violations while doing nothing to prevent terrorist attacks.

The same can be said for trying to use an algorithm to target foreign terrorists with lethal drone strikes:

---

[4] FBI Director Christopher Wray, A Review of the President's Fiscal Year 2025 Budget Request for the Federal Bureau of Investigation, Statement Before the Senate Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, D.C., June 4, 2024. Available online at https://www.fbi.gov/news/testimony/a-review-of-the-president-s-fiscal-year-2025-budget-request-for-the-federal-bureau-of-investigation.

[5] See Government Accountability Office, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159, November 2013 and *Aviation Security: TSA Does Not Have Valid Evidence Supporting Most of the Revised Behavioral Indicators Used in Its Behavior Detection Activities*, GAO-18-608R, July 2017. Available online at https://www.gao.gov.

[6] Government Accountability Office, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159, November 2013.

[7] Murtaza Hussein and Cora Currier, "U.S. Military Operations Are Biggest Motivation for Homegrown Terrorists, FBI Study Finds," *The Intercept*, October 11, 2016. Available online at https://theintercept.com/2016/10/11/us-military-operations-are-biggest-motivation-for-homegrown-terrorists-fbi-study-finds/

https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan

Given the multiple, well-publicized examples of U.S. lethal drone strikes in Afghanistan that killed innocent civilians vice Taliban terrorists, I see no need to rehash that history now. Suffice it to say that any AI system that would purport to be able to distinguish between a wedding party and a terrorist caravan should be viewed with the greatest skepticism.

In a domestic terrorism context, let's consider the following scenario:

An FBI agent opens an "Assessment" (which under current AG Guidelines requires no criminal predicate to initiate) on a particular individual that a confidential human source (CHS) being run by the agent has flagged for the Bureau's attention. The agent then feeds into their AI tool the following data derived from commercial and classified databases, physical surveillance notes and photography of the subject of the Assessment, and reports from a CHS:

Commercial database information: Assessment target purchased, within the same two-week period, the following items: an LWRC AR-15, 1000 rounds of NATO 5.56mm ammunition from the AmmunitionDepot.com, and from Amazon a copy of *The Turner Diaries* and *The Anarchist Cookbook*.

Classified database information: Utilizing FISA Section 702 database queries and queries of other currently non-public knowledge classified databases, the agent finds that the subject has been in contact with at least one other individual previously convicted of felonies and misdemeanors in connection with the January 6, 2021, attempted insurrection.

Physical surveillance notes: The agent conducted physical surveillance of the subject at a recent gun show in which the subject was in conversation with several firearms vendors, as well as individuals with either known membership in or association with the white supremacist group known as Patriot Front (PF).

Confidential Human Source data: The CHS, who is himself a member of PF, reported to his agent/handler that the subject of the Assessment was targeted for recruitment by the local leader of PF and that the conversation between the subject and the PF leader at the gun show ended cordially, with the subject telling the PF leader, "Let me get back to you on this."

After evaluating the information, the AI tool suggests to the FBI agent that the subject of the Assessment "may be on the path to radicalization" and that further, more invasive investigation of the individual is likely warranted.

In reality, the subject of the Assessment is a university student working on their PhD in domestic violent extremism. The student comes from a family with a multi-generational history of lawful gun ownership. The book purchases are part of the student's research program.

What evidence can the FBI and IC writ large provide at this point that any AI system they might deploy in a CT context--whether foreign or domestic--will not make the kind of false positive errors we've already seen in the real world, and which may be repeated in the future?

3. *What should effective performance metrics look like for the use of AI by the Intelligence Community (IC)?*

In the operational support to CT context, can AI get false positive and false negative rates down below the level of human error?

Can AI get false positive and false negative rates down to zero or near zero?

4. *What standards does the IC use in evaluating whether IC tools are ready to deploy in operational contexts? Are those the right standards?*

Because said standards are not available to the public, a truly independent, peer review-style appraisal of those standards is not currently possible.

5. *What new threats are created by AI's use by adversaries or malicious actors?*

Influence operations, identity theft.... the list is almost endless. The true challenge will be creating technology and techniques to surface malign actor AI use in a timely, actionable fashion.

6. *What privacy or civil liberties risks does the use of AI exacerbate?*

Increased problematic use of AI combined with facial recognition technology leading to false arrest is clearly a major, extremely serious threat.

Another threat is the potential use of an AI system to sift through existing digital law enforcement and/or IC databases. We have already seen how employees at FBI and NSA have improperly searched stored data on Americans. How much more serious could that problem become when AI is involved?

7. *How might bias, non-transparency, or unreliability in AI systems harm individuals? How can that harm be detected or mitigated?*

I'll pose a related question that I believe will help answer the one posed by the Board:

How might AI be harnessed to 1) ingest all applicable statutes, case law, and internal department/agency directives/orders/guidance and then 2) conduct searches of SENTINEL, SENTINEL GOLD, and any other FBI databases containing stored data and case files on U.S. Persons (as defined in statute) to determine whether or not individual special agents, supervisory special agents, section chiefs, unit chiefs, and other managers and lawyers responsible for ensuring adherence to the Bill of Rights, related statutes, case law, and internal regulations/guidance are, in fact, adhering to the law?

If--and I emphasize if--an AI tool of the kind I've described could be created to assist the DoJ and NSA IG's with ensuring DoJ and NSA personnel's compliance with surveillance statutes and case law, might the kinds of abuses we've witnessed with the FISA Title I (Woods Procedures) and Title VII (Section 702) authorities be dramatically reduced and inspection/audit completion accelerated?

8. *What recourse do people or agencies have if AI malfunctions or is otherwise proven unreliable?*

If DoJ or any other department or agency have developed such redress procedures, I have not seen public versions of them. I would point out that the debacle that is the TSA "No Fly List" is clearly an example of how ***not*** to approach redress issues.

9. *Can IC analysts ever be sure that AI augmented analysis is correct?*

I'll answer that question with a question: Can an AI system be successfully trained to use the concepts and methods behind alternative competing hypotheses (ACH)?
Finally, I'd like to raise a possible use of AI that could dramatically alter for the better U.S. government classification and declassification practices.

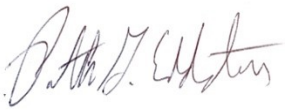
Columbia University history professor Matthew Connelly's declassified document analysis project, known as History Lab[8], utilizes a form of AI to scan declassified federal records to find patterns in the material that provide a level of insight not previously possible in the field of history. His most recent book, *The Declassification Engine: What History Reveals About America's Top Secrets*,[9] was featured at a Cato Institute event in September 2023 that I strongly encourage the Board to review.[10]

Connelly and his team have used a form of AI to actually uncover evidence of programs and activities that, to their knowledge, remain classified to this day. Now, consider the possibility of building an AI system that could ingest all extent declassified materials in agency/department electronic reading rooms and from other sources, then run searches against 1) existing classified holdings and 2) pending FOIA requests to see if still-classified material should be declassified and to expedite FOIA responses to requesters. Such a system could assist in protecting legitimate, current secrets as well as making available to the public records that should've been declassified and released years, even decades, earlier.

I thank the Board for soliciting public comment on this critical issue.

Sincerely,

[8] Available on line at http://history-lab.org/. See also Connelly's website at https://www.matthewconnelly.net/.
[9] Matthew Connelly, *The Declassification Engine: What History Reveals About America's Top Secrets* (New York: Pantheon, 2023).
[10] https://www.cato.org/multimedia/events/declassification-engine-what-history-reveals-about-americas-top-secrets.



Patrick G. Eddington
Senior Fellow
Cato Institute