

*Comment of the*  
**CENTER FOR AI AND DIGITAL POLICY**  
*to the*  
**PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD**  
*in response to*  
**NOTICE OF A PCLOB PUBLIC FORUM EXAMINING THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERTERRORISM AND REQUEST FOR PUBLIC COMMENT**

July 1, 2024

We write to you on behalf of The Center for AI and Digital Policy (“CAIDP”) in response to the Notice and Request for Public Comment<sup>1</sup> (“NRPC”) issued by the Privacy and Civil Liberties Oversight Board (“PCLOB”) relating to the upcoming public forum examining the role of artificial intelligence in counterterrorism.

CAIDP is an independent research and education non-profit based in Washington, DC and Brussels.<sup>2</sup> Our global network of AI policy experts and advocates advise national governments and international organizations on artificial intelligence and digital policy, including the OECD, European Union, the Council of Europe, G7, G20, UNESCO, and various branches of the U.S. Government. We also publish the annual *Artificial Intelligence and Democratic Values Report*, providing a comprehensive review of AI policies and practices in 80 countries.<sup>3</sup>

We address specific questions in the NRPC in our comments below. Our overarching recommendations to the PCLOB are to exercise its oversight authority<sup>4</sup> to ensure that:

1. Pseudoscientific and human-rights violating technologies in counter-terrorism and national security measures are prohibited
2. Safeguards and mitigation measures in accordance with the Guidance of the Office of Management and Budget<sup>5</sup> (OMB) are built into AI systems used for counterterrorism and national security efforts

---

<sup>1</sup> Privacy and Civil Liberties Oversight Board, *Notice of a PCLOB Public Forum Examining the Role of Artificial Intelligence in Counterterrorism and Request for Public Comment* (May 23, 2024), Federal Register, <https://www.federalregister.gov/documents/2024/05/23/2024-11317/notice-of-a-pclob-public-forum-examining-the-role-of-artificial-intelligence-in-counterterrorism-and>.

<sup>2</sup> CAIDP, *About* (2024), <https://www.caidp.org/about-2/>.

<sup>3</sup> CAIDP, *Artificial Intelligence and Democratic Values* (2024), <https://www.caidp.org/reports/aidv-2023/>.

<sup>4</sup> 42 U.S.C. § 2000ee, <https://www.congress.gov/108/statute/STATUTE-118/STATUTE-118-Pg3638.pdf>

<sup>5</sup> Office of Management and Budget (OMB), *Advancing governance, innovation, and risk management for agency use of artificial intelligence*, Memorandum for the Heads of Executive Departments and Agencies, (Mar. 28, 2024), <https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf> [OMB AI Guidance]

3. The Department of Homeland Security addresses conflicts of interest regarding tech company members of the AI safety and security board who also participate in the federal procurement process
4. Generative AI systems are not considered critical infrastructure<sup>6</sup>

### **Recommendation 1: Prohibition of pseudoscientific and human-rights violating technologies in counter-terrorism and national security measures**

The PCLOB should review AI systems that are pseudoscientific and violate fundamental rights. PCLOB should recommend that these systems are prohibited.

#### ***i. Predictive risk assessments in policing and immigration***

Models that claim to predict future behavior,<sup>7</sup> such as criminal recidivism or even the identity and location of a crime, are pseudoscientific technologies that draw spurious, often discriminatory,<sup>8</sup> correlations that are leveraged by authorities under claims of “objectivity” and “science.”<sup>9</sup> In fact, a 2020 letter by more than 1500 mathematicians called to end predictive policing work,<sup>10</sup> but such algorithms continue to be deployed and lead to unlawful and incorrect decisions.<sup>11,12</sup> The PCLOB must advise against the use of predictive policing technologies in counterterrorism efforts as the scientific basis for this technique is not clearly established.

#### ***ii. Facial recognition technology***

The use of facial recognition technology (“FRT”) for mass surveillance threatens the rights to privacy, consent, and transparency.<sup>13</sup> To be effective at identifying persons of interest, FRT systems must also collect data on and track movements of many more individuals who have no relation to the given crime.<sup>14</sup> FRT is also flawed due to racial and gender disparities in its

---

<sup>6</sup> Ryan Heath, *Exclusive: OpenAI's Chris Lehane says AI is "critical infrastructure"*, Axios, (Apr. 25, 2024), <https://www.axios.com/2024/04/25/openai-chris-lehane-ai-critical-infrastructure>

<sup>7</sup> Will Douglas Heaven, *Predictive policing algorithms are racist. They need to be dismantled.*, MIT Technology Review (July 17, 2020), <https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/>.

<sup>8</sup> David Arnold, Will Dobbie, and Peter Hull, *Measuring Racial Discrimination in Algorithms*, Becker Friedman Institute for Economics at the University of Chicago (2021), <https://www.aeaweb.org/articles?id=10.1257/pandp.20211080>.

<sup>9</sup> CAIDP, *Statement to Senate Judiciary Committee on “AI in Criminal Investigations and Prosecutions”*, [https://www.linkedin.com/posts/center-for-ai-and-digital-policy\\_caidp-statement-sjc-ai-and-justice-jan-activity-7155812624608215040-7C5p](https://www.linkedin.com/posts/center-for-ai-and-digital-policy_caidp-statement-sjc-ai-and-justice-jan-activity-7155812624608215040-7C5p)

<sup>10</sup> Lilah Burke, *Mathematicians Urge Ending Work With Police*, Inside Higher Ed (June 23, 2020), <https://www.insidehighered.com/news/2020/06/24/mathematicians-urge-cutting-ties-police>.

<sup>11</sup> Matt Stroud, *Heat Listed*, The Verge (May 24, 2021), <https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list>.

<sup>12</sup> Robert Koulisch & Kate Evans, *Punishing With Impunity: The Legacy of Risk Classification Assessment in Immigration Detention*, 36 Georgetown Immigration Law Journal pp. 1-72 (2021), [https://scholarship.law.duke.edu/faculty\\_scholarship/4115/](https://scholarship.law.duke.edu/faculty_scholarship/4115/).

<sup>13</sup> CAIDP, *Ban Facial Surveillance Technology*, <https://www.caidp.org/statements/ban-facial-surveillance-technology/>

<sup>14</sup> Nicol Turner Lee & Caitlin Chin-Rothmann, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color* (2022), <https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>.

accuracy.<sup>15</sup> Blindly trusting the outputs of FRT systems in law enforcement has resulted in incorrect and appalling incarceration.<sup>16,17</sup> Currently, the Transportation Security Administration (“TSA”) verifies passenger identity through FRT and travelers must proactively opt out of the system to be screened manually.<sup>18</sup> A bi-partisan group of lawmakers have also recently petitioned Senate majority and minority leaders to restrict the use of facial recognition technology by TSA and have highlighted that the potential misuse of such technologies expand far beyond security checkpoints.<sup>19</sup> As a recent report from the National Academies found:

“Facial recognition technology intersects with equity and race in several key ways. Many systems deployed in the U.S. are trained using datasets that are imbalanced and disproportionately rely on data from White individuals. As a result, these systems have higher false positive match rates for racial minorities. They also provide law enforcement with a powerful new surveillance tool that can serve to reinforce patterns of or perceived need for elevated scrutiny, especially in marginalized communities, which may be compounded through law enforcement’s use of reference galleries based on mug shots. These issues create additional burdens for some groups of individuals, including African Americans and others that have been historically marginalized in the U.S.”<sup>20</sup>

### ***iii. Biometric categorization***

Attempts to categorize people according to race, gender, nationality, religion, sexual orientation, ideology, etc. based on biometric data are fundamentally pseudoscientific. These attempts to map biometrics onto subjective social constructs are problematic. Biometric systems can also have particularly harmful effects on minority groups, such as transgender people.<sup>21</sup>

### ***iv. Sentiment detection and analysis***

---

<sup>15</sup> Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Conference on Fairness, Accountability, and Transparency, 81 Proceedings of Machine Learning Research pp. 1-15 (2018), <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

<sup>16</sup> Kashmir Hill and Ryan Mac, ‘Thousands of Dollars for Something I Didn’t Do’, The New York Times (updated April 6, 2023), <https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html>.

<sup>17</sup> Benj Edwards, *Innocent pregnant woman jailed amid faulty facial recognition trend*, ArsTechnica (August 7, 2023), <https://arstechnica.com/information-technology/2023/08/innocent-pregnant-woman-jailed-amid-faulty-facial-recognition-trend/>.

<sup>18</sup> Edward Graham, *How TSA’s opt-outs for biometric screenings informed White House AI policy*, Nextgov (April 10, 2024), <https://www.nextgov.com/emerging-tech/2024/04/how-tsas-opt-outs-biometric-screenings-informed-white-house-ai-policy/395626/>.

<sup>19</sup> Letter to Senator Chuck Schumer and Senator Mitch McConnell, (May 2, 2024), [https://www.merkley.senate.gov/wp-content/uploads/2024\\_05\\_02\\_LTR-TSA-Freeze-to-Leadership.pdf](https://www.merkley.senate.gov/wp-content/uploads/2024_05_02_LTR-TSA-Freeze-to-Leadership.pdf)

<sup>20</sup> National Academies of Sciences, Engineering, and Medicine, *Advances in Facial Recognition Technology Have Outpaced Laws, Regulations; New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns* (Jan. 17, 2024), <https://www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns>

<sup>21</sup> Connor O’Sullivan, *Unmasking AI’s Detrimental Effects on the Trans Community*, Medium: Towards Data Science (June 20, 2023), <https://towardsdatascience.com/unmasking-ais-detrimental-effects-on-the-trans-community-d8f870949d79>.

Systems that claim to detect emotions, thoughts, or truthfulness from physical features, conversations, and expressions are pseudoscientific and discriminatory.<sup>22</sup> Research shows that the expression of emotions varies depending on the situation and cultural context.<sup>23</sup> These may also discriminate against people with disabilities, such as facial disorders, disfigurement, autism, or social anxiety.

Several of these techniques are already prohibited by the EU AI Act.<sup>24</sup> As the European Parliament explained:

The new rules ban certain AI applications that threaten citizens' rights, including biometric categorisation systems based on sensitive characteristics and untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases. Emotion recognition in the workplace and schools, social scoring, predictive policing (when it is based solely on profiling a person or assessing their characteristics), and AI that manipulates human behaviour or exploits people's vulnerabilities will also be forbidden.<sup>25</sup>

The Court of Justice of the European Union has also determined that machine learning systems that produce outcomes that cannot be meaningfully contested may not be used for decision-making concerning fundamental rights.<sup>26</sup> A related provision on Transparency and Explainability in the influential OECD AI Principles, now adopted by over 50 countries including the United States, states that operators of AI systems should “enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.”<sup>27</sup>

The European Data Protection Supervisor and the European Data Protection Board have called several ‘red lines’ for AI deployment, including a general ban on biometric identification for surveillance or discrimination and emotion detection.<sup>28</sup> And the former UN High

---

<sup>22</sup> Merve Hickock, *Comments of Merve Hickok to the Office of Management and Budget (OMB) regarding the Draft Memorandum published in Federal Register 88 FR 75625*, (November 4, 2023).

<sup>23</sup> Tuan Le Mau, et al., *Professional actors demonstrate variability, not stereotypical expressions, when portraying emotional states in photographs*, 12 *Nature Communications* 5037 (August 19, 2021), <https://doi.org/10.1038/s41467-021-25352-6>.

<sup>24</sup> European Parliament, *Artificial Intelligence Act: MEPs adopt landmark law* (March 13, 2024), <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law>

<sup>25</sup> *Id.*

<sup>26</sup> *Ligue des droits humains*, C-817/19 (CJEU 2022).

<sup>27</sup> Marc Rotenberg, *CJEU PNR Decision Unplugs the ‘Black Box,’* *European Data Protection Law Review* Volume 8, Issue 3 (2022), pp. 431 – 435, DOI: <https://doi.org/10.21552/edpl/2022/3/15>

<sup>28</sup> European Data Protection Board, *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination* (2021) [https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible\\_en](https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en)

Commissioner for Human Rights Michelle Bachelet has called for a ban on AI applications that do not comply with international human rights law.<sup>29</sup>

At the very least, the PCLOB should make known that other democratic nations are establishing clear prohibitions on AI systems that lack a scientific basis or violate fundamental human rights. The PCLOB should encourage the adoption of similar prohibitions in the United States.

**Recommendation 2: Establish safeguards and mitigation measures counterterrorism and national security AI systems in accordance with the OMB guidance for AI systems deployed by the federal government**

National security systems have been exempted from President Biden’s Executive Order on Safe, Secure, and Trustworthy AI<sup>30</sup> and from the OMB AI Guidance. National security systems which include everything from domestic intelligence programs to autonomous systems are exempted from the OMB Guidance.<sup>31</sup> The PCLOB has a critical role to play in filling this vacuum. The Board must exercise its oversight authority to ensure that rights-impacting AI systems are not deployed and entrenched in counter-terrorism and national security efforts. In particular, the board should address the following:

***i. Bias mitigation***

Following the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy championed by the United States, “states should take proactive steps to minimize unintended bias in military AI capabilities.”<sup>32</sup> The PCLOB must advocate for bias mitigation measures to be built into every AI system deployed for the purposes of counter-terrorism and national security. This includes but is not limited to training data that adequately represents various identity groups and data labeling which accounts for existing social biases.

***ii. Fail switch, or ability to disengage deployed systems***

The Declaration also urges a mechanism for “disengaging or deactivating deployed systems, when [AI] systems demonstrate unintended behavior.”<sup>33</sup> When AI systems are not operating as expected toward a clearly defined goal, it is critical they possess a fail switch,

---

<sup>29</sup> UN Human Rights, Office of the High Commissioner, *Artificial intelligence risks to privacy demand urgent action – Bachelet* (2021), <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E>; See also Center for AI and Digital Policy, ‘UN Urges Moratorium on AI that Violates Human Rights’ (2021) <<https://www.caidp.org/app/download/8343909663/CAIDP-Up-date-2.34.pdf>; See also, Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values* (2022) <<https://www.caidp.org/reports/aidv-2021/>>.

<sup>30</sup> Executive Order 14110 of October 30, 2023, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Federal Register Vol. 88, No. 210, pg. 75191-75226, <https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf>

<sup>31</sup> Faiza Patel, *An Oversight Model for AI in National Security: The Privacy and Civil Liberties Oversight Board*, Brennan Center for Justice, (Apr. 30, 2024), <https://www.brennancenter.org/our-work/analysis-opinion/oversight-model-ai-national-security-privacy-and-civil-liberties>

<sup>32</sup> U.S. Department of State, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, (November 9, 2023), <https://www.state.gov/wp-content/uploads/2023/10/Latest-Version-Political-Declaration-on-Responsible-Military-Use-of-AI-and-Autonomy.pdf>.

<sup>33</sup> *Ibid.*

especially when human lives are at stake. The PCLOB—in the legislative and oversight processes—must ensure each deployment of an AI system in national security efforts has a means of manual deactivation. The termination obligation is the ultimate statement of accountability for an AI system and presumes that systems must at all times remain within human control. Where that is not possible, the system itself should be terminated.<sup>34</sup>

### ***iii. Auditability***

According to the Declaration, AI systems must possess “methodologies, data sources, design procedures, and documentation that are transparent to and auditable by relevant defense personnel.”<sup>35</sup> The PCLOB must ensure processes for the auditing of training data and algorithms and evaluation of standards set forth by the Declaration. Ex-ante impact assessments that consistently evaluate how these systems affect various identity groups are necessary to ensure bias is recognized and minimized.<sup>36</sup> Rigorous documentation and disclosure of training data is critical for meaningful evaluation and developing techniques to minimize bias and harm.

### **Recommendation 3: Seek explanation from the Department of Homeland Security on the AI Safety and Security Board**

As it stands, 13 of the 22 members of the DHS Artificial Intelligence Safety and Security Board<sup>37</sup> represent corporate interests. The Board’s tilt toward those that would profit from government contracts and minimal regulation of AI products, in the case of national security even exempt from OMB guidance, is deeply troublesome. If DHS seeks to fairly evaluate public concerns of implementing AI systems into counterterrorism and national security efforts, the DHS should establish clear measures to address conflicts of interest that would arise from the corporate/industry members on its Board. The PCLOB should recommend published conflict of interest statement for all members of the AI Safety and Security Board, propose increased representation from civil society groups and academic institutions, and seek explanation of the measures DHS will implement to address conflicts of interest stemming from federal procurement of AI systems developed and marketed by the corporate members on its board.

### **Recommendation 4: Closely monitor claims for generative AI systems to be considered critical infrastructure**

---

<sup>34</sup> CAIDP, *The Universal Guidelines for AI*, Principle 12: Termination Obligation, <https://www.caidp.org/universal-guidelines-for-ai/>

<sup>35</sup> Ibid.

<sup>36</sup> CAIDP Comments on NIST Risk Management Framework Following White House Executive Order, (Feb. 2, 2024), [https://www.caidp.org/app/download/8500506063/CAIDP%20Comments\\_NIST%20RFI\\_88%20FR%2088368\\_02022024.pdf](https://www.caidp.org/app/download/8500506063/CAIDP%20Comments_NIST%20RFI_88%20FR%2088368_02022024.pdf); CAIDP Statement to Office of Management and Budget on the AI Guidance for Federal Agencies, (Dec. 5, 2023), <https://www.caidp.org/app/download/8494694763/CAIDP-Statement-Canada-COE-01102024.pdf>

<sup>37</sup> DHS, *Artificial Intelligence Safety and Security Board*, <https://www.dhs.gov/artificial-intelligence-safety-and-security-board>

Executives of generative AI companies have been pushing to include AI within the scope of critical infrastructure. CISA’s AI Roadmap identifies “responsible use of AI” as its first line of effort.<sup>38</sup> The PCLOB must exercise its oversight authority and regularly review national security agencies roadmap and use-cases to ensure that these programs do not create a pathway for generative AI systems to be categorized as critical infrastructure. Generative AI systems pose serious risks to public safety and national security – from enabling cybersecurity attacks to election interference and disinformation.<sup>39</sup> PCLOB should exercise oversight as to the specific mitigation measures being implemented to ensure that integration of generative AI products with national security systems and critical infrastructure is not providing “threat actors” with “increased attack surfaces.”<sup>40</sup>

Finally, we urge PCLOB to continually maintain meaningful public comment opportunities. As per our analysis of 80 countries in our *Artificial Intelligence and Democratic Values Index*, we have found that the comment process in the US on AI policy is not typically meaningful.<sup>41</sup> We specifically recommend that PCLOB carry forward the recommendations of the comments received, including these recommendations from the Center for AI and Digital Policy, or provide a “reasoned explanation” for its decision not to adopt the recommendations received.

We thank PCLOB for this opportunity to provide our comments on AI governance and the role of PCLOB. We look forward to your response to our recommendations.

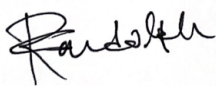
Sincerely,



Merve Hickok  
CAIDP President



Marc Rotenberg  
CAIDP Executive Director



Christabel Randolph  
CAIDP Associate Director



Samir Duggasani  
CAIDP Research Assistant

---

<sup>38</sup> CISA, *Roadmap for Artificial Intelligence 2023-2024*, [https://www.cisa.gov/sites/default/files/2023-11/2023-2024\\_CISA-Roadmap-for-AI\\_508c.pdf](https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdf)

<sup>39</sup> CAIDP, *Supplementary Complaint to FTC re OpenAI and ChatGPT*, (Jul. 10, 2023), para. 67-82, <https://www.caidp.org/cases/openai/>; Jack Aldane, *Agencies ‘don’t have the tools’ to head off ChatGPT threat to national security, warns Pentagon’s AI Chief*, Global Government Forum (May 11, 2023), <https://www.globalgovernmentforum.com/agencies-dont-have-the-tools-to-head-off-chatgpt-threat-to-national-security-warns-pentagons-ai-chief/>

<sup>40</sup> Daniel M. Gerstein & Erin N. Leidy, *Emerging Technology and Risk Analysis: Artificial Intelligence and Critical Infrastructure*, RAND Corporation (April 2, 2024), [https://www.rand.org/pubs/research\\_reports/RRA2873-1.html](https://www.rand.org/pubs/research_reports/RRA2873-1.html).

<sup>41</sup> CAIDP, *Artificial Intelligence and Democratic Values* (2024), <https://www.caidp.org/reports/aidv-2023/>.