Statement of Patrick Toomey
Deputy Director, National Security Project, American Civil Liberties Union
U.S. Senate AI Insight Forum: National Security
December 6, 2023

Senators, thank you for inviting me to this AI Insight Forum. I am the Deputy Director of the National Security Project at the American Civil Liberties Union (ACLU), where I lead our work on artificial intelligence (AI) and national security. The ACLU is eager to support policymakers' efforts to ensure that the foundational tenets of nondiscrimination, equal protection, and due process are at the heart of governmental uses of AI, including by national and homeland security agencies involved in law enforcement, intelligence, and defense. These uses of AI are among the federal government's most advanced, opaque, and consequential. Although national security agencies have rapidly deployed AI, enforceable safeguards for civil rights and civil liberties have barely taken shape. Congress must fill this gap before flawed systems are entrenched and continue to harm the American people. Even more immediately, Senators should strongly urge President Biden and leaders of national security agencies to adopt the kinds of baseline protections that the President has ordered outside of national security and intelligence.

I. A Two-Tiered Approach to Regulating AI, with Lower Protections for National Security Uses, Exposes Already-Marginalized Communities to Further Harm

It should be a truism that all arms of the federal government are subject to foundational principles of nondiscrimination, equal protection, and due process. Unfortunately, the emerging framework for regulating governmental uses of AI has not applied those principles evenly across the government. Instead, policymakers have opted for a two-tiered approach, seeking to establish robust safeguards for AI used by most government agencies, while embracing sweeping exemptions and carve-outs for "national security systems," intelligence agencies, and defense agencies, subjecting them to a separate, to-be-determined policy.[1]

This approach is misguided. As described below, national security agencies are using AI systems in contexts such as surveillance, watchlisting, border searches and detention, biometrics, and immigration benefits – contexts where AI can cause significant harm to people in the United States. Moreover, these activities disproportionately impact already-marginalized populations, such as immigrants and racial and religious minorities. National security agencies have raced ahead of other federal agencies in their development and deployment of AI, but broad exceptions for national security will delay the adoption of critical rights and privacy safeguards. Instead, equivalent protections should be provided by such agencies wherever possible – especially for AI applications that impact people in the United States – with rules permitting calibration of those requirements only for specific use-cases where an exception is strictly justified by national security needs and subject to robust oversight. Congress should reject the current two-tiered approach and take the lead in establishing strong safeguards for homeland security, intelligence, and defense uses of AI.

[1] *E.g.*, Advancing American AI Act, Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7225(d), 7228, here (exempting the Department of Defense and intelligence agencies); Executive Order 14110 of October 30, 2023, sec. 4.8, 88 Fed. Reg. 75191, 75204 (Nov. 1, 2023) (exempting "national security systems"); OMB, Draft Memorandum: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (Nov. 1, 2023), here [hereinafter "OMB Draft Memorandum"] (similar).

II. Use of AI by National Security Agencies Harms People in the United States

The use of AI by national security agencies presents some of the greatest harms and risks for people in the United States. Congress should regulate these AI systems accordingly. More than two years ago, a sweeping report by the congressionally-mandated National Security Commission on AI (NSCAI) left no question that U.S. intelligence agencies and the military are integrating 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 and questioning at the border, and who it labels a "risk" or "threat" to national security.[2] In many of these areas, the deployment of AI appears to be well underway. But the public knows next to nothing about AI deployed by the country's largest law enforcement and intelligence entities like the Department of Homeland Security, Federal Bureau of Investigation, National Security Agency, and Central Intelligence Agency, and even less about the safeguards that exist – if any. And just as in areas like policing and the criminal legal system, these algorithmic systems threaten to perpetuate discrimination and racial profiling, while endangering Americans' civil rights and liberties. Based on the limited public information available, we highlight several examples below.

DHS's Automated Targeting System and Algorithmic Predictions. Several DHS systems rely on secret algorithms to make predictive judgments and identify individuals for heightened government scrutiny or investigation. At the heart of these systems is the Automated Targeting System (ATS), which relies on secret rule sets, in combination with biographic and other data, to assess whether individuals pose a "threat" to national security, and can lead to prolonged border detentions, intrusive searches, and unexplained visa denials.[3] DHS components utilize ATS for programs like ATLAS and Continuous Immigration Vetting to conduct risk assessments of travelers, evaluate applicants seeking immigration benefits, identify potential instances of fraud, or pursue denaturalization cases, among other applications.[4]

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.[5] There is no public information about how ATS makes its predictions, no empirical data about its reliability or effectiveness, and no notice to individuals who are adversely impacted by its determinations. At the same time, there are significant concerns that ATS relies on data reflecting long-entrenched biases against racial and religious minorities, including the federal government's terrorism watchlists, some of which are composed predominantly or disproportionately of Muslim individuals.[6] As the NSCAI warned more than two years ago, Congress must ensure that DHS's "automated screening processes lead agents only to the information they need and are authorized to access, and do not impermissibly single out individuals based on characteristics such as race or religion."[7]

---

[2] NSCAI, Final Report 143-45 (2021) [hereinafter NSCAI Final Report], here.
[3] DHS, Privacy Impact Assessment Update for the Automated Targeting System (2017), here; Rachel Levinson-Waldman & José Guillermo Gutiérrez, *Overdue Scrutiny for Watch Listing and Risk Prediction*, Brennan Ctr. for Just. (Oct. 19, 2023), here.
[4] *See, e.g.*, DHS, Privacy Impact Assessment for ATLAS (2020), here.
[5] Rachel Levinson-Waldman & José Guillermo Gutiérrez, *DHS Must Evaluate and Overhaul its Flawed Automated Systems*, Just Security (Oct. 19, 2023), here.
[6] *Id*.
[7] NSCAI Final Report at 143-53, 395-410, here.

Social Media Surveillance, Sentiment Analysis, and Risk Scoring. Documents obtained by the ACLU and others reveal widespread federal agency efforts to monitor and exploit social media information using AI and algorithmic tools, including by DHS. These tools – often purchased from private, third-party vendors – claim to apply AI to social media posts and other data to conduct "sentiment analysis," identify "derogatory" information about individuals, and assign "risk scores."[8] At least some of the tools are used to scrutinize U.S. citizens and permanent residents in addition to refugees and asylum seekers.[9] Almost nothing is known about these systems' specific data sources and the biases they may contain; what criteria or algorithms are used to gauge "sentiment," flag so-called "derogatory" information, or assign risk scores; or how the resulting information is used by DHS agents or other officials. But in a sign of where systems like these may be headed next, one company recently demonstrated a tool that relies on ChatGPT to conduct sentiment analysis of social media posts.[10]

Such surveillance raises grave First Amendment concerns and has repeatedly been shown to have questionable or "no value."[11] Suspicionless monitoring of online activity intrudes on individuals' ability to associate freely, chills protected speech, and disproportionately affects racial and religious minorities. Analyzing social media is notoriously difficult, given the sheer volume of information and the ease of misinterpreting individuals' online messages – especially for agencies like DHS, which vets travelers who hail from hundreds of countries and speak thousands of languages. Reviews of DHS's social media surveillance concluded that it has not "adequately demonstrated the practical utility of collecting this information" and found little, if any, effectiveness.[12] This use of AI – with no transparency, testing, or other basic protections – heightens the danger that social media monitoring will be misused, with severe repercussions for racial and religious minorities and those engaged in protected speech and association online.

NSA Intelligence Collection and Analysis. U.S. intelligence agencies like the NSA have used AI "for a very long time" to support their signals intelligence programs, and today they are seeking "ubiquitous AI integration in each stage of the intelligence cycle."[13] They may use these tools to help select new surveillance targets, to perform natural language processing of intercepted voice calls and text, and to analyze the vast amounts of communications they vacuum up every day – often ensnaring Americans.[14] All of these activities carry significant risks of

---

[8] Joseph Cox, *The A.I. Surveillance Tool DHS Uses to Detect 'Sentiment and Emotion'*, 404 Media (Nov. 25, 2023), here; Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees*, Vice Motherboard (May 17, 2023), here; Joseph Cox, *Inside ICE's Database for Finding 'Derogatory' Online Speech*, 404 Media (Oct. 24, 2023), here; Joseph Cox, *'Night Fury': Documents Detail DHS Project to Give 'Risk Scores' to Social Media Users*, Vice Motherboard (Jun. 6, 2023), here.

[9] *See supra* note 8; Ken Dilanian, *DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media*, NBC News (May 10, 2021), here.

[10] Lucas Ropek, *ChatGPT Is Apparently a Great Surveillance Tool*, Gizmodo (Nov. 17, 2023), here.

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

[12] *See, e.g.*, OIRA, Notice of Office of Management and Budget Action ICR Reference No. 202007-1601-001 (Apr. 2, 2021), here; Brennan Center for Justice & Electronic Privacy Information Center, Comment re: Social Media Collection on ESTA, OMB Control No. 1651-0111 (Mar. 25, 2022), here.

[13] NSA, *GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT* (Sep. 21, 2023), here; NSCAI Final Report at 110.

[14] NSCAI Final Report at 108-18; NSA, *Artificial Intelligence: Next Frontier is Cybersecurity* (July 23, 2021), here; Jay Stanley, *Will ChatGPT Revolutionize Surveillance?*, ACLU (Apr. 19, 2023), here.

causing or compounding privacy intrusions. For example, built-in bias or flawed intelligence algorithms may lead to additional surveillance and investigation of individuals, exposing their lives to wide-ranging government scrutiny under FISA or other authorities. Yet few basic facts about these AI systems and their impacts are publicly known, notwithstanding an Inspector General evaluation of the NSA's use of AI that began in 2021.[15] The results of that comprehensive review should be released to the public in a declassified form.

Facial Recognition and Video Analytics. National and homeland security agencies have widely experimented with and deployed AI-powered facial recognition tools.[16] For example, 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 video collections."[17] 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.

Facial recognition technology, however, disproportionately misidentifies and misclassifies people of color, trans people, women, and members of other marginalized groups.[18] In the law enforcement context, facial recognition has repeatedly led to the false arrest and wrongful incarceration of Black people.[19] The use of such tools for national security purposes raises the high likelihood of similar problems with accuracy, bias, and discrimination. Facial classification algorithms, which can purportedly assess anything from an individual's emotional state to their level of threat in a crowd, also suffer from serious error rates.[20] And it can be extremely difficult to correct these inaccuracies even with human review, as humans' cognitive bias toward trusting machine-generated outputs can lead investigators or analysts to ignore credible contradictory evidence.[21] Moreover, concerns would persist even if inaccuracies were resolved: an expanding apparatus of facial recognition technology will make a vast network of surveillance possible, threatening freedom of association and speech, due process, and privacy.

III. Congress Should Urge the President and National Security Agencies to Adopt Existing Baseline Protections Immediately

Congress should urge the President and national security agencies to provide the baseline protections already being developed in other federal agencies. 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, lacking meaningful transparency and accountability mechanisms or binding rules. For example, ODNI's *Principles for Artificial Intelligence Ethics for the Intelligence Community* describes six high-level guidelines – including a commitment to

[15] DOD & NSA Inspectors General, Mem. for the DNI re: Announcement of Joint Evaluation (Aug. 6, 2021), here.
[16] *See, e.g.*, ACLU, Comment re: DHS Information Collection Request (Dec. 6, 2021), here.
[17] Drew Harwell, *FBI, Pentagon Helped Research Facial Recognition for Street Cameras, Drones*, Wash. Post. (Mar. 7, 2023), here.
[18] *See, e.g.*, Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems*, Wash. Post (Dec. 19, 2019), here; Joy Buolamwini et al., *Gender Shades*, MIT Media Lab, here.
[19] *See* Letter from ACLU to Hon. Kamala Harris, Vice President of the United States, at 3 n.9 (Aug. 3, 2023), here.
[20] *See, e.g.*, Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions* (Dec. 6, 2018), here; Kate Crawford, *Artificial Intelligence Is Misreading Human Emotion*, The Atlantic (Apr. 27, 2021), here.
[21] Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, New Yorker (Nov. 13, 2023), here.

be "transparent and accountable" – but the public to date has seen little evidence of either.[22] The Defense Department recently released a toolkit "to help DoD personnel design, develop, deploy, and use AI systems responsibly," but using the toolkit is voluntary.[23]

Given the slow development – let alone implementation – of vitally necessary civil rights, civil liberties, and privacy safeguards by national security agencies, Congress should urge the President to ensure that AI used by these agencies is subject to the same fundamental standards as other AI uses. For example, the President might extend the protections outlined in OMB's Draft Memorandum on "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" to national security agencies. The Draft Memorandum outlines baseline risk-management practices for AI that impacts the rights or safety of individuals or communities. The Draft Memorandum correctly identifies rights- and safety-impacting AI as including surveillance-related risk assessments, facial matching, location monitoring, decisions related to immigration or asylum, risk assessments of individuals entering the United States, control of physical movements, and control of the movement of vehicles.[24] Those uses must be documented in public inventories and are subject to minimum risk-management practices, such as assessing the AI's impact prior to deployment and mitigating its risks. Because the Draft Memorandum currently exempts national security systems and intelligence agencies from its scope, Congress should urge the President to fundamentally change that approach.

The NSCAI recommended that national security agencies adopt similar protections, including risk assessments for AI's impact on free expression, equal protection, and privacy.[25] Its final report also urged national security agencies to increase transparency around AI through more robust Privacy Impact Assessments and System of Record Notices to provide a "holistic picture" about AI and its collection, use, and storage of personal information. Yet those recommendations have been ignored. Congress should urge the President to adopt them.

Congress should lead in urging the President and national security agencies to mandate the baseline protections described above, with modifications only for specific use-cases strictly – and publicly – tailored to identified national security needs. And if necessary, Congress should pass legislation to achieve that goal.

We appreciate your consideration, and if you or your staff have any questions, please do not hesitate to contact us.

Sincerely,

Patrick Toomey
Deputy Director, National Security Project
ACLU

---

[22] ODNI, *Intelligence Community Principles of Artificial Intelligence* (2020), here; ODNI, *Artificial Intelligence Ethics Framework for the Intelligence Community* (2020), here.
[23] Department of Defense, *CDAO Releases Responsible AI (RAI) Toolkit for Ensuring Alignment With RAI Best Practices* (Nov. 14, 2023), here.
[24] OMB Draft Memorandum at 11-12, 20.
[25] NSCAI Final Report at 396-97.