AI Insight Forum: National Security

Statement of Faiza Patel
Senior Director, Liberty and National Security Program
Brennan Center for Justice at NYU School of Law
December 6, 2023

Majority Leader Schumer, Senators Rounds, Heinrich and Young:

Thank you for the concerted attention you have brought to bear on the important questions raised by artificial intelligence (AI). The Brennan Center has worked for a decade on issues at the intersection of AI and national security, particularly the use of these tools by intelligence, homeland security, and law enforcement agencies. We have found scant publicly available evidence of the efficacy of many of these tools and considerable evidence of their risks to Americans' privacy, civil rights, and civil liberties.

We appreciate that Congress and the administration have taken steps to increase transparency, trust, and fairness in AI tools in many areas. But national security has largely been exempted from these developments. If Americans are to trust the government's use of AI tools for national security—especially where such uses directly affect them—this must change. The important principles articulated by Congress in the Advancing American AI Act and in President Biden's executive order on AI should extend to highly consequential national security programs. 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. Below we set forth our key concerns and recommendations.

1. Exclusion of National Security from AI Regulatory Development

The 2022 Advancing American AI Act entirely exempts the Intelligence Community (IC) from its requirements. It excuses the Department of Defense from preparing and maintaining use case inventories. Other agencies are required to make use case inventories public but only "to the extent practicable and in accordance with applicable law and policy, including those concerning the protection of privacy and of sensitive law enforcement, national security, and other protected information"—a limitation that can too easily defeat transparency. President Biden's 2023 Executive Order 14110 on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" maintains these exclusions and adds an additional and expansive exception for "national security systems" as defined in 44 USC 3552(a)(6)(A), which covers all intelligence activities and classified systems. EO 14110 directs the preparation of a separate memorandum for these systems, but there is little publicly available information about the parameters and process for this effort. These three sets of exceptions—for the IC and the Defense Department; for sensitive law enforcement, national security, and other protected information; and for national security systems—are also reflected in the draft memorandum on "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," published by the Office of Budget and Management (OMB) on November 3, 2023 ("Draft OMB Memorandum"). As a result of these three interlocking sets of rules:

- National security systems are outside the purview of the chief AI officers charged with overseeing evaluations of AI systems and mitigating risks to rights and safety.
- There is no public transparency for IC and Defense systems, national security systems, or those containing sensitive law enforcement, national security, or other protected information. Even

programs about which information has already been released—e.g., in Congressional testimony, systems of records notices, or privacy impact assessments—do not have to be disclosed.
- The IC and national security systems are exempt from OMB minimum practices meant to ensure that AI is effective, accurate, fair, and rights-respecting.
- Chief AI officers may waive minimum practices for systems containing sensitive law enforcement, national security, and other protected information if they find the requirement would "create an unacceptable impediment to critical agency operations." This creates a significant loophole because the standard is likely to be too easily met in practice and, because waivers are not publicly reported, it undermines transparency.

2. Excluded Systems Pose Serious Risks to Privacy, Rights, and Liberty

The draft OMB memorandum includes a list of rights-impacting uses of AI that require safeguards. The IC and other federal agencies already run AI-enabled programs in several of these rights-impacting areas and are accelerating their development of these technologies. Below, we discuss two such program areas which demonstrate the acute risks of leaving national security systems out of AI regulation.

a. Social Media Monitoring

The Department of Homeland Security (DHS) runs at least 12 social media monitoring programs. Too often these efforts target First Amendment protected speech and political and social movements. At the same time, the government's own analyses show that they rarely achieve their stated objectives.

For example, DHS's Office of Intelligence and Analysis (I&A)—which is a member of the IC—combs through Americans' social media in search of threats. It also scoops up information about Americans' political and personal views with no discernable connection to DHS missions. In 2020, I&A used social media and other information to assemble dossiers on racial justice protestors to share with law enforcement and circulated terrorism bulletins about journalists' tweets. It deployed a tool called Tangles, which claims to use natural language processing and other AI technology to make inferences, such as the "sentiments" expressed by people, and to map out protestors' online footprint and those of their friends and family. As documented in a 2021 review by the DHS Office of the General Counsel, the program suffered from deep problems, ranging from pressure to generate intelligence in support of the Trump administration's political messaging to a lack of understanding of the difference between protected speech and threats. The next year, despite a change in administration and leadership, the DHS inspector general found that I&A "does not have comprehensive policies and procedures to ensure [that] its employees effectively collect [open source intelligence] and adhere to privacy protections."

Nonetheless I&A has plowed ahead, announcing that it will mine the internet and social media searching for "narratives" that it claims could lead to violence—although it has never explained how it chooses some among a multitude of narratives to target, connects them to violence, or distinguishes between true threats and the type of anonymous hyperbole that is all too common online. For example, I&A monitored Americans' online reactions to the Supreme Court's decision overturning *Roe v. Wade*, which it speculated have the potential to generate national security threats. Notably, many of the views that DHS believes are of concern are shared by tens of millions of Americans—e.g., concerns about the Covid vaccine—allowing the unit to sweep up a huge volume of core political speech with no clarity on how it parses posts to identify actual threats.

Social media monitoring has failed time and again to identify actual threats. DHS's general counsel's report found that officers collecting social media to identify emerging threats instead gathered material on "a broad range of general threats," ultimately yielding "information of limited value." In the context of vetting refugees, a 2016 DHS brief concluded that social media "did not yield clear, articulable links to national security concerns, even for those applicants who were found to pose a potential national security threat based on other security screening results." A 2017 DHS inspector general audit of the same programs found that the department had not even bothered to measure their effectiveness. Most recently, intelligence officials charged with using social media handles to vet visa applicants concluded that doing so added "no value" to the screening process and had "very little impact" on its accuracy.

The analyses generated by I&A's online monitoring influence law enforcement decisions far beyond DHS. Disseminated to tens of thousands of police around the country, its reports influence resource allocation, help develop targets and priorities, and provide justification for surveillance and, in some cases, prosecution. For example, I&A used social media monitoring—among other intelligence methods—to develop and share an assessment labeling criticism of environmental damage and "anti-law enforcement sentiment" domestic violent extremist "narratives," which it claims have spurred on a nationwide epidemic of terrorism. Georgia officials have cited DHS characterizations to support a sweeping racketeering indictment of 61 protestors and arrested 42 for domestic terrorism.

And I&A is only expanding its footprint in AI-powered monitoring tools. In June 2023, DHS updated a privacy impact assessment for its data analysis tools to include natural language processing and machine learning. I&A is charged with developing these tools to analyze DHS's vast data holdings for its own operations and to enable parts of the department to do so as well. Documentation about these tools is subject to review by DHS civil rights, legal, and privacy staff, but these offices have traditionally been easily overruled based on operational concerns and in any event are not charged with undertaking, nor equipped to conduct, the type of rigorous evaluation required for AI.

This is exactly the type of program that should be made to meet the minimum practices set out in the Draft OMB Memorandum

b. Facial Recognition

Facial recognition technology poses extreme risks to privacy, civil rights, and civil liberties. Our faces, like our fingerprints, are unique to each of us. But unlike other biometric information, our faces are visible as we live our daily lives and when we share pictures online for our friends and family and thus easily captured in government and private databases.

Multiple studies show that AI-powered facial recognition systems are inaccurate, particularly for people of color and the record of law enforcement agencies use of these tools indicates that they exacerbate racial bias in policing. A 2022 empirical study by criminal justice scholars at Georgia State University found that police's use of facial recognition contributes to greater racial disparity in arrests. Politico reviewed some 11 months' worth of facial recognition requests by the New Orleans police, finding that the technology was almost always used on Black persons. Incorrect matches have resulted in multiple wrongful arrests, overwhelmingly of Black people. When used for intelligence gathering—for example, to identify individuals at a political protest—facial recognition undermines constitutional rights to free speech and assembly. And based on law enforcement's use of this technology, it is likely to result in bias-infected results.

Despite these risks, agencies like the Federal Bureau of Investigation (FBI)—which is part of the IC—raced to adopted facial recognition technology. As of 2019, through its Next Generation Identification (NGI) database and its arrangements with other agencies, the FBI had access to over 640 million face photos. It has also contracted with Clearview AI, a company that scrapes photos from the internet without consent and has claimed that by 2023 it will have captured 100 billion facial photos. The Bureau has deployed this technology without adequate testing, training, and safeguards.

A series of reports by the Government Accountability Office (GAO) document the FBI's lax approach towards its facial recognition technology. In a 2016 report, GAO set out two metrics for the accuracy of facial recognition technology: the detection rate (i.e., how often the technology generates a match when a person is in its database) and the false positive rate (i.e., how often the technology incorrectly generates a match to a person in its database. But the FBI only tested the system's detection rate in one scenario, leaving out other circumstances in which it can, and has, been used. And the FBI did not test its system's false positive rate, on the theory that the system only generates leads, not actual identifications, and thus there were no false positives. This, as GAO points out, "presents an incomplete view of the system's accuracy." Since the FBI's system generates up to 50 potential matches, the agents reviewing results must exercise considerable judgement. But, according to a 2023 GAO report, almost all FBI agents using the Clearview AI facial recognition tool were not trained in its use, and the Bureau did not have in place policies specific to facial recognition technology to mitigate risks to civil rights and civil liberties. In a further illustration of the FBI's careless approach, a 2021 GAO report shows that the FBI did not even track the external facial recognition systems used by its employees, and thus could not even assess and mitigate the risks of using them.

The FBI also uses facial recognition for intelligence and national security purposes. It has disclosed its use of these tools to search for persons associated with open assessments. These are broad intelligence gathering efforts, which 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. In addition, FOIA documents show that the Bureau worked with the Defense Department to develop technology that could be used to identify people from video footage captured by street cameras and flying drones. The 2021 GAO report shows that this system "in development" at the FBI and according to the agency is currently being used for research and education purposes. It is not too difficult, however, to anticipate its use for monitoring protests, especially recalling the agency's 2020 activation of counterterrorism teams to hunt for supposed antifa terrorists among racial justice protestors.

These risks are magnified with the advent of new forms of AI. Law enforcement agents have already been caught editing photos submitted for facial recognition and tools that make manipulation of images easier makes such practices even more likely and further undercuts the reliability of the technology. And the addition of other types of AI, such as emotion and gait recognition, which are unproven but which agencies such as the FBI and DHS are reportedly using or exploring, only magnifies existing potential for mischief.

The FBI's facial recognition system—and the American public on whom it is used—would surely benefit from the transparency, testing, and rights safeguards of the Draft OMB Memorandum.

3. Recommendations

The examples above show how security agencies collect and process Americans' data, track our behavior and movements, and even act based on computer-generated analyses with little regard for effectiveness and de minimis safeguards. As EO 14110 notes, new AI tools will only make it easier to "extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires," magnifying the risks to Americans' privacy and freedoms of speech and assembly, and bolstering bias. Congress must act to ensure that the use of new technologies in consequential and secret national security applications does not sweep away our constitutional values. We urge Congress to take the following steps:

Apply AI Principles to National Security Systems. Congress should make a clear statement that the framework articulated in EO 14110 and the Draft OMB Memorandum should apply to the IC and to national security systems. Algorithmic systems that have such serious impacts on our privacy, civil rights and civil liberties should be demonstrably safe, effective, and fair.

Establish Independent Oversight of the Privacy and Civil Liberties Impacts of AI. Congress should either expand the mandate and resources of the Privacy and Civil Liberties Oversight Board (PCLOB) to cover non-counterterrorism uses of AI or stand up a new body dedicated to addressing the privacy and civil liberties impacts of AI systems. PCLOB has provided the public with valuable insights into some of the government's most secretive counterterrorism programs, as well as advising agencies such as DHS and the FBI. A counterpart for AI is sorely needed.

Enact Comprehensive Privacy Legislation. As many lawmakers have noted, comprehensive privacy legislation is essential to mitigating the risks of AI. Such legislation should cover the government acquisition, use, and dissemination of data from third parties and include strict standards for when such information may be accessed and utilized by intelligence, homeland security, and law enforcement agencies.

Increase Transparency. Use case inventories with specific requirements overseen by an entity like OMB can provide important transparency but are not required for national security systems. Several agencies issue systems of records notices and privacy impact assessments, which can provide insight into the use of AI. However, these notices are not required for many national security systems. Even when issued, they generally do not provide a holistic picture of how programs operate and how different systems interact. Moreover, too often this information is made available long after the system is in operation and notices are skipped for new applications on the theory that they are covered by earlier notices. The data mining reports required for federal programs involving data analysis aimed at uncovering patterns that are meant to predict terrorist or criminal activity provide a useful model for supplementing mechanisms such as use case inventories and privacy documentation.

Ensure Due Process. Redress for decisions taken by agencies like DHS and FBI is already very weak. The black box nature of AI systems will only exacerbate this failing, leaving Americans with little recourse when they are subject to measures triggered by algorithms, including when AI is used as part of building a case for prosecution. Congress should require DHS and the FBI and other agencies whose use of national security AI affects Americans to undertake a review of their redress procedures and develop robust and accessible mechanisms that take account of the agencies' use of AI. These should be evaluated and approved by the Attorney General for consistency with constitutional principles of due process.