Testimony of Jake Laperruque
Deputy Director, Security and Surveillance Project at the Center for Democracy & Technology
For the U.S. House of Representatives Committee on Homeland Security
Hearing Entitled "Advancing Innovation (AI): Harnessing Artificial Intelligence to Defend and Secure the Homeland."
May 22, 2024

Chairman Green, Ranking Member Thompson, and members of the House Homeland Security Committee, thank you for the opportunity to testify on the important topic of how we can ensure that use of artificial intelligence ("AI") enhances America's national security and protects human rights and core democratic values.

I am Jake Laperruque, Deputy Director of the Security and Surveillance Project at the Center for Democracy & Technology ("CDT"), a nonprofit, nonpartisan organization that defends civil rights, civil liberties, and democratic values in the digital age. For nearly three decades, CDT has worked to ensure that rapid technological advances promote our core values as a democratic society.

AI is rapidly altering the world, offering both exhilarating possibilities and alarming risks. It's critical to examine how it should be used in fields where the stakes are highest, such as homeland security. AI can support our goals, but only if we use it properly. While AI capabilities can often prove remarkable, we are wielding complex software systems, not a magic wand. For AI to foster safety and protect our rights, it must be used in a responsible manner. In this testimony I describe key principles for doing so, examine facial recognition as a case study into why responsible use of AI is so critical, and provide a set of steps Congress can take to promote effective use of AI technologies in the national security space.

I. Responsible Use and Well-Designed Safeguards Are Essential if AI is to Aid National Security and Uphold Our Constitutional Values

In order to provide benefits rather than cause harm, AI must be used in a careful and responsible manner. Government use of AI needs at its foundation a set of governance principles, which in turn lead to the development of concrete rules governing AI's acquisition and use. If AI is not developed and deployed responsibly, it will lead our agencies and investigators astray in situations where avoiding errors is most critical. For example, imagine a predictive AI system that was designed to generate leads, but was built on selective or biased training data; such a system will cause investigators to waste time and resources chasing bad leads, leaving genuine security dangers unattended to. Or consider a facial recognition system programmed so poorly that it frequently triggers false alarms, leading investigators not to register the needed level of concern when a real threat appears amid the noise.[1]

[1] See, e.g. Lizzie Dearden, "Facial Recognition Wrongly Identifies Public as Potential Criminals 96% of Time, Figures Reveal", *The Independent*, May 7, 2019, https://perma.cc/YZ36-RC6A.

In addition to bolstering security, responsible use of AI is critical to upholding our constitutional values. AI — especially in the context of government use and national security — is often framed as an "Arms Race." But we must take care in what we're racing towards. Authoritarian regimes in China, Russia, and Iran have all shown how AI can be used to throttle dissent, oppress marginalized groups, and supercharge surveillance.[2] The United States must not recklessly rush ahead with the single-minded goal of deploying AI only to replicate these anti-democratic systems. Truly winning the "AI Arms Race" does not mean simply achieving the fastest buildup on the broadest scale. It requires deployment in a manner that reflects and advances America's constitutional values.

We are at a time of public anxiety and uncertainty about AI. Securing the trust of the American people and our global allies — as well as maintaining an advantage over adversaries — can only be achieved if we demonstrate that this technology will both be effective and support civil rights, civil liberties, and democratic values.

II. Principles for Ensuring Responsible Use of AI Technologies

The Department of Homeland Security ("DHS") has taken a positive step in highlighting the need for responsible use of AI in its recently published AI Roadmap, and offering principles for doing so.[3] Notably, the Roadmap commits to its use of AI being "rigorously tested," "safeguard[ing] privacy, civil rights, and civil liberties," and being "transparent and explainable." It is critical that DHS and other government agencies that use AI for national security purposes adhere to and build upon these and other key principles.

Principles for responsible use of AI technologies should be applied broadly across development and deployment. In particular, government use of AI should be:

1. Built upon proper training data;
2. Subject to independent testing and high performance standards;
3. Deployed only within the bounds of the technology's designed function;
4. Used exclusively by trained staff and corroborated by human review;
5. Subject to internal governance mechanisms that define and promote responsible use;
6. Bound by safeguards to protect human rights and constitutional values; and
7. Regulated by institutional mechanisms for ensuring transparency and oversight.

Training Data. Proper training data is the first hurdle to avoiding "garbage in, garbage out" problems with AI. The effectiveness of AI systems depends on the data used to develop them. If data is inaccurate or of poor quality, then the resulting system trained from it will exhibit flaws. Training data does not even need to be wrong to cause problems - training AI on selective and unrepresentative data can warp how

---

[2] Paul Mozur, "In Hong Kong Protests, Faces Become Weapons", *N.Y. Times*, July 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html; Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", *N.Y. Times*, Apr. 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *N.Y. Times*, July 8, 2018, https://perma.cc/27U7-S365; Lena Masri, "Facial Recognition is Helping Putin Curb Dissent With the Aid of U.S. Tech", *Reuters*, Mar. 28, 2023, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/; Khari Johnson, "Iran to Use Facial Recognition to Identify Women Without Hijabs", *Ars Technica*, Jan. 11, 2023, https://arstechnica.com/tech-policy/2023/01/iran-to-use-facial-recognition-to-identify-women-without-hijabs/.

[3] Dept. of Homeland Security, *Artificial Intelligence Roadmap 2024* (2024), https://perma.cc/Y6KQ-5J9V.

those AI systems later function. For example, a common flaw discovered in facial recognition systems was use of training sets that were disproportionately white and male; as a result these systems displayed algorithmic bias in which women and people of color were misidentified at far higher rates.[4]

Independent Testing. Requiring independent testing and high performance standards is a key safeguard against adoption of low quality systems. Such measures are important because poor algorithm design or flawed training data are not always readily apparent, and AI technologies are frequently being applied to new situations and circumstances. Testing should be conducted by independent experts, with transparent methodology that allows for peer review and improvement. Testing should occur periodically, and should be a precondition for procurement, as well as regularly conducted for AI systems already in use. And critically, systems should be tested in real-world contexts (e.g., in pilots or limited releases), using the same system settings as will be used in actual deployments, and using real-world scenarios. As those system settings or scenarios change or evolve, testing should evolve to account for them.

Deploy Only for Designed Function. Deploying AI technologies only within the bounds of the technology's designed functions is a principle that takes on several components. This requires making sure that "input data" — meaning the data and requests that AI technologies analyze and base their outputs on — is proper. It must be high quality, which can be challenging as input data often exists on a sliding scale and depends upon a huge range of factors, and cannot simply be labeled "good data, use it" or "bad data, toss it." For example, as discussed in detail below, a wide range of factors impact whether an image can be effectively scanned by facial recognition technology.[5]

Assessing whether certain data and tasks properly fit within an AI technology's designed capabilities can also be hard to discern. For example, as CDT has discussed, automated social media analysis tools can be undone when tasked with reviewing posts that contain slang, sarcasm, and other context-specific language.[6] AI can also be deployed egregiously beyond the bounds of the technology's designed functions. It is critical that the government not treat AI technologies as a philosopher's stone that can turn lead into gold — if a system is tasked with analyzing poor quality data or given tasks beyond its designed function, it will produce unreliable results.

Training and Human Review. The often challenging nature of evaluating the proper bounds for using an AI technology highlight why training and human review is another essential principle. If staff using AI are not specifically trained in how it should be deployed, poor results will follow. Training is also necessary for preventing automation bias — meaning the tendency for people to naturally assume automated systems are correct, even in the face of conflicting evidence — in general, and in particular for effectively gauging how much weight to give results from AI in various situations. And even when AI is used in the most favorable settings, accuracy cannot be guaranteed, making human review and corroboration of results essential. Human review is important not only to account for naturally occurring

---

[4] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Fairness, Accountability and Transparency, Proceedings of Machine Learning Research 81:77-91 (2018), https://perma.cc/C9FV-G5SY; Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Standards and Technology (2019), https://doi.org/10.6028/NIST.IR.8280.

[5] See Section III.

[6] Mana Azarmi, "The U.S. Government is Demanding Social Media Information From 14.7 Million Visa Applicants – Congress Should Step In", Center for Democracy & Technology, Jul. 3, 2019, https://perma.cc/JMK8-BA7B.

errors in AI systems, but also to guard against risk of malicious tampering that degrades results.[7] Further, human approval should be required before AI systems are used to take specific actions that may affect individuals' rights (e.g., targeting a person for surveillance).

Internal Governance. Agencies should put in place internal governance mechanisms to promote responsible use of AI. The recently released Office of Management and Budget's (OMB) guidance on governance and risk management for federal agencies' use of AI is an important step forward in advancing this goal.[8] That OMB memo should serve as a baseline for the forthcoming National Security Memorandum that is intended to establish parallel guidance for national security systems. The OMB guidance provides useful direction to agencies concerning internal governance processes in support of responsible and transparent use of AI technologies. Agencies should clearly assign decision-making and internal oversight responsibilities, including requirements for approval by high-level officials for procurement of systems and use cases that present particularly high risks. Legal, civil rights, and privacy officials should be part of the decision making process through the AI development, procurement, and deployment lifecycle and have comprehensive visibility into how departments and agencies are using AI.

Effective governance also requires clear standards for procurement of AI technologies from third-party vendors.[9] Standards should include requirements for pre-award government evaluation of vendors' AI models to reject vendors whose models don't address the needs agencies identify.[10] Standards should also include contractual requirements for vendor reporting with sufficient detail to support agencies' ongoing independent review of model performance, evaluation of and reporting on impacts, and agencies' own disclosures in their AI inventories.[11]

Safeguarding Rights. While the principles above largely focus on ensuring AI is as accurate and efficacious as possible, it is also essential that AI technologies are used in a manner that upholds constitutional values, civil rights, and civil liberties. Safeguards for achieving this cannot merely consist of generally tasking agencies or individual staff with abiding by broad principles, and hoping that AI's use will be properly restrained on a case-by-case basis

Agencies should conduct impact assessments to determine whether an AI system risks being biased or otherwise violating constitutional and human rights. Certain AI technologies or uses should be prohibited because they pose an unacceptable risk to rights (e.g., AI profiling or risk scoring systems that attempt to predict an individual's future criminality). As the OMB memorandum notes, "[w]here the AI's risks to rights or safety exceed an acceptable level and where mitigation is not practicable, agencies must stop using the affected AI as soon as practicable." In cases where a system poses risks that can be mitigated, agencies should impose specific and concrete rules tailored to each specific AI technology and its use scenarios. For example, agency guidelines on use of facial recognition should account for image quality

[7] See Section V.

[8] Office of Management and Budget, *M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (Mar. 28, 2024), https://perma.cc/RKK7-SMYJ. See also, Center for Democracy & Technology, "CDT Welcomes Final OMB Guidance on Federal Agencies' Use of AI, and Now Looks Toward Earnest Implementation", Mar. 28, 2024, https://perma.cc/MQ34-VUWG.

[9] Hannah Quay-de la Vallee et al, Center for Democracy & Technology, *The Federal Government's Power of the Purse: Enacting Procurement Policies and Practices to Support Responsible AI Use* (2024), https://perma.cc/BL2L-5Z6M.

[10] *Id.* at 37-39.

[11] *Id.* at 39-40, 42-45.

in various ways, and strictly regulate what (if any) adjustments may be made to an image prior to scanning. Agency rules must be designed to promote both efficacy and protection of civil rights, civil liberties, and constitutional principles. While agency rules are an essential first step, Congress should also bolster protections with statutory safeguards as needed for AI technologies that present significant risks to civil rights and civil liberties.

Transparency & Oversight. Upholding responsible use will require mechanisms for transparency, oversight, and accountability. Such efforts must be institutionalized systems, rather than ad hoc review. Oversight structures should exist within agencies, and across the federal government. Systems should also be designed to facilitate public review and input, which is important for fostering trust, ensuring compliance with rules, and promoting improvements in how AI technologies are used. This will be challenging in terms of use of AI in national security spheres where secrecy is the norm, but this cannot be an excuse for inaction. Section IV of this testimony proposes certain measures Congress could take that are specifically designed to account for the secrecy of national security operations while promoting public engagement.

III. Facial Recognition as a Case Study of Why Responsible Use Is Key for Both Security and Democratic Values

Facial recognition serves as a premiere example of why responsible use of AI technologies is critical to ensuring safety as well as civil rights and civil liberties, and why the principles described above serve as the foundation for responsible use. Facial recognition is especially fitting in evaluating responsible use because it is an AI technology that the government has used for law enforcement and security purposes for roughly a decade.[12] Facial recognition can provide a roadmap of why key principles are essential, as well as offer clear warnings about how irresponsible and careless uses undermine public safety.

AI technologies are too often viewed more as magic than software. This problem has occurred in practice with facial recognition, which is sometimes treated as universally applicable and virtually infallible. For example, major facial recognition vendors have reportedly included marketing materials and user instructions that improperly claim the technology won't produce false matches, will provide definitive identifications rather than candidate lists, and can be used on low-quality images without impairing results.[13] Clearview AI — which, despite its notoriety, is used by 10 federal law enforcement entities

---

[12] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy and Technology, Oct. 18, 2016, https://www.perpetuallineup.org/.

[13] Jake Laperruque, "Key Facts About Face Recognition for Policymaking", Project on Government Oversight, Aug. 24, 2021, https://perma.cc/VBW6-Q44G.
("Tech Vendors' Exaggerations About How Face Recognition Functions:
Claim: According to Clearview AI, "you will almost never get a false positive. You will either get a correct match or nor [sic] results." Fact: Any system, no matter how advanced its algorithm, can produce false positives.
Claim: FaceFirst stated, "Facial recognition gives officers the power to instantly identify suspects. … "… Officers can simply use their mobile phones to snap a photograph of a suspect from a safe distance. If that individual is in their database it can then positively identify that person in seconds with a high degree of accuracy."
Fact: Field conditions for this scenario — such as lighting, angle, and distance — significantly increase the likelihood of misidentifications.
Claim: DataWorks Plus pitched its systems as tech that "uses facial recognition technology to positively match photos of an individual" with capabilities such as "discovering a person's identity during investigations."
Fact: Face recognition can offer sets of possible matches, but should not be relied on to offer a definitive, positive match.
Claim: Matches with low confidence thresholds can be acceptable. Amazon worked with police to develop a system that will always "return the top 5 leads based on confidence levels" (meaning the Amazon-recommended setting will return matches no matter how low the confidence threshold is) and touted the fact that police are "willing to trade a lower confidence level for more leads."

including Customs and Border Protection and Immigration and Customs Enforcement[14] — went so far as to post advertisements to police networks claiming that law enforcement officials would "realize you were the crazy one" for not expecting face recognition to function the same as in absurd TV depictions like "NCIS, CSI, Blue Bloods."[15] These claims are not just untrue; they encourage law enforcement to engage in unsafe practices and build investigations around unreliable, low-quality marches.

In reality, facial recognition's effectiveness is highly variable, and depends upon a range of factors. First, the reliability of facial recognition depends upon the quality of images being scanned; images with low lighting, bad resolution, poor angles, or obstructions are much less likely to yield reliable matches.[16] This is a prime example of how AI is only as good as the data it interacts with. There is no clear line that separates "good usable images" and "bad unusable images" into two neat groups. Rather, there is a gradation based on all the image-quality factors listed above, each of which has a huge range; evaluating how much value to give to matches from photos across that range can be highly difficult.

Accuracy of facial recognition is also impacted by the significant variance in how effective different facial recognition systems are based on factors such as overall quality of the training data, as well as degree of algorithmic bias. While some systems claim to have overcome demographic variance in accuracy, for others it is a huge problem; a National Institute of Science and Technology study found certain systems were up to *100 times more likely* to misidentify Asian and African American people than white men.[17] Low quality training data — in particular, using databases of faces that are demographically skewed — is the main source of this problem.[18]

System settings impact the quality of results as well. Many law enforcement entities, including the FBI, configure systems to *always* return a set of potential matches for a facial recognition scan, no matter how reliable (or unreliable) those matches are.[19] Such practices inevitably yield matches that are undependable, but might be interpreted as a credible lead from highly sophisticated AI technology.

Fact: Using an unrestricted setting that always returns matches — no matter how low the confidence threshold — creates serious risk of misidentifications.
Claim: Clearview AI said, "A photo should work even if the suspect grows a beard, wears glasses, or appears in bad lighting."
Fact: Photo conditions that limit ability to scan facial features impact the ability to accurately obtain matches. Obstructions and low lighting make misidentifications more likely even for high performing systems.").

[14] Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518, at 12 (2021), https://www.gao.gov/assets/gao-21-518.pdf; see also Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, GAO-23-105607, https://www.gao.gov/assets/gao-23-105607.pdf (describing continued use of Clearview by at least six agencies).

[15] Jake Laperruque, "Correcting Misconceptions and Planning Effective Safeguards on Face Recognition Technology", Project on Government Oversight, Jul. 13, 2021, https://perma.cc/S7TT-Z85Z.

[16] See, *Artificial Intelligence and Human Rights: Hearing Before the Sen. Subcomm. on Human Rights and the Law of the Sen. Comm. on the Jud.*, 118th Cong. (2023) (testimony of Alexandra Reeve Givens, President and CEO, Center for Democracy & Technology), https://perma.cc/5ZKF-J97B; see also, The Constitution Project's Task Force on Facial Recognition Surveillance and Jake Laperruque, "Facing the Future of Surveillance", Project on Government Oversight, Mar. 4, 2019, https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance.

[17] Drew Harwell, "Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubts on Their Expanding Use", *Washington Post* (Dec. 19, 2019), https://perma.cc/8RJE-VBMH.

[18] See, "Joy Buolamwini: How Does Facial Recognition Software See Skin Color?", *National Public Radio: TED Radio Hour*, Jan. 26, 2018, https://www.npr.org/transcripts/580619086; see also Joy Buolamwini, "Unmasking the Bias in Facial Recognition Algorithms", MIT Sloan School of Management, Dec. 13, 2023, https://perma.cc/7J6P-JDG4.

[19] See, Erin M. Priest, Privacy and Civil Liberties Officer, FBI, "Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System," (2019), https://perma.cc/FR82-SFPB ("A gallery of two to fifty photos will be returned, with the law enforcement agency choosing the size of the gallery. If no choice is made, a default of twenty photos is returned").

Furthermore, it is disturbingly common for law enforcement to artificially replace portions of faces they are scanning; this practice injects further uncertainty and speculation into results.[20] Techniques for doing so range from using computer-generated imagery (CGI) to add pieces of a face not captured in photos, to replacing the real face entirely with a composite sketch or celebrity look alike.[21] This conduct puts the veneer of useful intel built from objective, high-tech tools onto shoddy and baseless results.

All of these factors demonstrate the need for rigorous guardrails on the design and use of face recognition technology. We have already seen the devastating effect that lax practices and overreliance on facial recognition can have on people's rights, with misidentifications that led to wrongful arrests, and jail time for innocent individuals.[22] Beyond the undue deprivation of liberty, these errors have caused lasting harms including loss of employment, enormous legal bills, and mental health issues.[23] Unfortunately, because the role of facial recognition investigations is often hidden, these incidents are likely just several among many instances in which poor applications of the technology have caused wrongful arrests.[24,25] Beyond the significant harm to the individuals improperly flagged as matches, reliance on facial recognition errors undermines public safety by leading investigations far afield, which could have especially severe consequences in the national security context.

Facial recognition also gives a dire warning to why responsible use is necessary to protect constitutional values. Absent strong safeguards, AI can supercharge anti-democratic practices, and severely harm civil rights and civil liberties. In China, facial recognition is used for surveillance on a mass scale, including to oppress the nation's Uigher populace.[26] The pervasive application of facial recognition in itself becomes a means for authoritarianism: By using facial recognition for low-level offenses such as jaywalking, the Chinese government creates a digital panopticon, threatening its people with the fear that the government,

---

[20] Clare Garvie, "Garbage In, Garbage Out | Face Recognition on Flawed Data", Georgetown Law Center on Privacy & Technology, May 16, 2019, https://perma.cc/D4BL-WQGU.

[21] James O'Neill, "How Facial Recognition Makes You Safer", *N.Y. Times*, June 9, 2019, https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html ("We have used editing software to substitute a generic feature when a suspect is closing his eyes or sticking out his tongue in the submitted photo. The system can also create a mirror image of the right side of a face if we have only the left side, for example, to produce a 3-D model"); Clare Garvie, "Garbage In, Garbage Out | Face Recognition on Flawed Data", Georgetown Law Center on Privacy & Technology, May 16, 2019, https://perma.cc/D4BL-WQGU ("One detective from the Facial Identification Section (FIS), responsible for conducting face recognition searches for the NYPD, noted that the suspect looked like the actor Woody Harrelson …. A Google image search for the actor predictably returned high-quality images, which detectives then submitted to the face recognition algorithm in place of the suspect's photo.")

[22] See, Khari Johnson, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives", *Wired*, Mar. 7, 2022, https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/; Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", *N.Y. Times*, Dec. 29, 2020, https://perma.cc/CHM4-QAZ3; Kashmir Hill and Ryan Mac, "'Thousands of Dollars for Something I Didn't Do,'" *N.Y. Times*, Mar. 31, 2023, https://perma.cc/CNK3-926N;
Johana Bhuiyan, "Facial Recognition Used After Sunglass Hut Robbery Led to Man's Wrongful Jailing, Says Suit," *Guardian*, January 22, 2024. https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit.

[23] See, Khari Johnson, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives", *Wired*, Mar. 7, 2022, https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/; Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", *N.Y. Times*, Dec. 29, 2020, https://perma.cc/CHM4-QAZ3; Kashmir Hill and Ryan Mac, "'Thousands of Dollars for Something I Didn't Do,'" *N.Y. Times*, Mar. 31, 2023, https://perma.cc/CNK3-926N.

[24] Khari Johnson, "The Hidden Role of Facial Recognition Tech in Many Arrests", *Wired*, Mar. 7, 2022, https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/; Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where it Falls Short", *N.Y. Times*, Jan. 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

[25] Disturbingly, it is likely that facial recognition misidentifications have caused innocent individuals not just to temporarily be held in jail but to actually face prison sentences, with charges based on erroneous matches leading to either wrongful conviction or accepting a plea bargain out of fear of long sentences or extended time in pretrial detention.

[26] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", *N.Y. Times*, Apr. 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *N.Y. Times*, July 8, 2018, https://perma.cc/27U7-S365.

empowered by AI, is always watching.[27] The governments in Russia and Iran also weaponize facial recognition to thwart dissent, with Russia deploying the technology against anti-war protesters and Iran using it to identify and threaten those demonstrating against the state's hijab mandate.[28]

Yet these disturbing and improper uses have not just occurred abroad — in the United States there are already documented instances of facial recognition being deployed against peaceful protesters.[29] This and other anti-democratic uses must not become the norm. Strong rules must be put into place to protect civil rights and civil liberties.[30]

Even though law enforcement use of face recognition is too often cloaked in secrecy, we at least know about the existence of this technology and have some insights into how government deploys it, and public interest researchers have been able to test and critique it. Unfortunately this is not the case with other AI products that may be in use. We do not have a broad list of AI technologies deployed in the national security space, let alone details on use that would allow us to effectively evaluate efficacy and risks. That is why it is essential that Congress consider the appropriate institutional mechanisms for ensuring transparency, oversight, and accountability.

IV. Congress Should Establish Institutional Oversight Measures to Support Responsible Use

Given its complexity and the range of technologies AI consists of, there will be no silver bullet for ensuring responsible use and adherence to the key principles outlined in this testimony. Instead, we should attempt to develop and continuously build on a broad set of policies that promote transparency, oversight, and accountability at a broad level, while vigorously working to enact and enforce specific regulations for each AI technology tailored to maximize its efficacy and adherence to democratic principles. In its recent AI Roadmap, DHS noted that responsible use of AI requires "continuous monitoring to build trust and accountability in AI applications," and the agency committed to establishing "safe, secure, and trustworthy use of AI by DHS through robust governance and oversight policies and practices."[31]

Congress should take steps in support of that goal through the measures discussed below. While these policies are important and we support their prompt adoption, they should not be viewed as comprehensive solutions. Promoting responsible use of AI will require continual engagement, review, and adaptation; this work must be done in consultation with a broad set of experts, impacted communities, and other stakeholders.

---

[27] Alfred Ng, "How China Uses Facial Recognition to Control Human Behavior", *CNET*, Aug. 11, 2020, https://perma.cc/P6Y3-U7XV ("The punishing of these minor offenses is by design, surveillance experts said. The threat of public humiliation through facial recognition helps Chinese officials direct over a billion people toward what it considers acceptable behavior, from what you wear to how you cross the street").

[28] Lena Masri, "Facial Recognition is Helping Putin Curb Dissent With the Aid of U.S. Tech", *Reuters*, Mar. 28, 2023, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/;
Khari Johnson, "Iran to Use Facial Recognition to Identify Women Without Hijabs," *Ars Technica*, Jan. 11, 2023, https://arstechnica.com/tech-policy/2023/01/iran-to-use-facial-recognition-to-identify-women-without-hijabs/.

[29] Joanne Cavanaugh Simpson and Marc Freeman, "South Florida Police Quietly Ran Facial Recognition Scans to Identify Peaceful Protestors. Is That Legal?", *Sun Sentinel*, June 26, 2021, https://www.sun-sentinel.com/2021/06/26/south-florida-police-quietly-ran-facial-recognition-scans-to-identify-peaceful-protestors-is-that-legal/.

[30] CDT has previously advanced a number of policy proposals to accomplish this goal, which we described in Section IV(d).

[31] Dept. of Homeland Security, *Artificial Intelligence Roadmap 2024*, at 15-16 (2024), https://perma.cc/Y6KQ-5J9V. .

a. Oversight Board for Use of AI and National Security

Development and enforcement of proper policies for responsible use of AI is especially challenging in the national security space because government operations in this realm are often shrouded in secrecy. Active investigations, tradecraft, and protection of sources and methods limit public knowledge. The level of secrecy due to these legitimate factors is compounded by overclassification.

As a flagship tool for ensuring responsible use in the face of this obstacle, Congress should create an oversight board for the use of AI in national security, modeled after the Privacy and Civil Liberties Board ("PCLOB"), established by the 9/11 Commission Act of 2007. This AI Oversight Board would be a bipartisan, independent entity within the executive branch, with members and staff possessing security clearances and given access to all use of AI within the national security sphere. The AI Oversight Board would be tasked with:

1) Serving as an overseer within classified settings to promote responsible use of AI. Such work would involve not only fostering compliance with existing rules, but also encouraging improved agency practices.
2) Facilitating greater public knowledge and understanding of uses of AI in the national security space, through development of reports and seeking viable declassification of relevant documents and information. In this work the AI Oversight Board should also solicit input of outside experts, affected communities, and other stakeholders. This would help building public trust, and serve as a conduit for outside expertise to improve use of AI in the national security space.
3) Provide policy recommendations to both the administration and Congress to better ensure that use of AI is responsible, aids security, and advances democratic values.

PCLOB demonstrates how effective this model can be for balancing the need for oversight with the secrecy built into national security space. Over the past 15 years, PCLOB has proven highly valuable in increasing public knowledge in the counterterrorism space, and thereby promoting better public policy for both security and civil liberties. For example, in 2014 PCLOB's report on use of the PATRIOT Act to conduct bulk collection of Americans' phone records demonstrated that despite its massive privacy harms, the program did not provide any meaningful counterterrorism value as its proponents had claimed.[32] This thorough and independent assessment of the program's efficacy was invaluable to the public debate over the bulk collection program, which Congress chose to outlaw the following year.[33]

PCLOB has also been greatly useful in relation to Section 702 of the Foreign Intelligence Surveillance Act. PCLOB has issued multiple reports on this warrantless surveillance authority, resulting in declassification of hundreds of pieces of information about the program, helping explain how certain operations under the law function, providing insights into the effectiveness and risks of various activities,

[32] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (2014), https://perma.cc/HS93-J5U3.

[33] See, Center for Democracy & Technology, "Victory: Passage of USA FREEDOM Act Reins in NSA Surveillance", Jun. 2, 2015, https://perma.cc/K6BC-X96A.

and included over a dozen policy recommendations.[34] This work had a significant positive impact on the recent public debate over Section 702's reauthorization that occurred over the past year.

We urge Congress to promptly establish an oversight board for use of AI in national security modeled after PCLOB in its structure, access to information, and obligations. Amd although we believe PCLOB provides an insightful roadmap, we also recommend Congress consult with PCLOB and other stakeholders on what institutional features could be adjusted to improve this new AI Oversight Board's effectiveness, as well as what distinctions might be necessary to better support its focus on AI.

b. Robust Transparency and Reporting Structure

While internal agency rules are necessary, they are far from sufficient to ensure responsible use of AI, especially given the secrecy of national security activities. Transparency and public awareness are a baseline for maintaining compliance by agencies and continued improvements in policy. The AI Oversight Board discussed above will contribute to this goal, but should not be laden with the full responsibility for achieving it. Congress should build institutionalized transparency and reporting structures into government use of AI for national security in at least two ways.

First, Congress should require declassification review of key documents on use of AI for national security. This should include all AI Impact Assessments, as well as Privacy Impact Assessments, Human Rights Impact Assessments, or Privacy Threshold Analyses conducted in relation to AI technologies. Required declassification review should also apply to agency guidelines for use of AI technologies, and legal analyses regarding use of AI systems. Finally, it should include any efficacy assessments of AI systems. Following the model of required declassification review for significant FISA Court opinions that Congress enacted as part of the USA FREEDOM Act in 2015, reviews should be conducted in a timely manner, and, if significant redactions that might impair understanding of the document are included, be accompanied by an unclassified summary.

Second, Congress should require annual agency reporting on use of AI technologies. These reports should include information describing: 1) the type of AI technologies used; 2) the types of data being analyzed by each AI technology used; 3) the types of government activities each AI technology is used for; 4) the number of individuals impacted by AI technologies and nature of that impact; and 5) the number of criminal, immigration, and administrative court proceedings in which evidence obtained or derived from AI technologies was submitted into evidence. The Office of the Director of National Intelligence Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities — composed largely of data Congress required be reported annually as part of the USA FREEDOM Act — could be instructive in developing these annual reports on use of AI technologies, especially as they are used in the national security context.

c. Build Institutional Mechanisms Into Funding

[34] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2023), https://perma.cc/M73R-ZK4D; Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014) https://perma.cc/S5KV-88GL.

Given the pace of development and the stakes of this issue, the government must not deploy AI technologies now and plan to develop best practices and sort through mistakes later. As Congress considers upcoming funding for new applications of AI in the national security realm, it should require that agencies adopt institutional mechanisms such as those described above as part of their governance of AI development and deployment. If Congress does not take such steps now, we may find ourselves too far behind to keep up with developments and ensure responsible use.

d. Establish statutory safeguards for the most rights-impacting AI technologies

While agencies should institute impact assessments and internal guidelines to protect civil rights and civil liberties, Congress should also supplement these rules with statutory protections, particularly for AI technologies that pose the most significant risks to individual rights. Self-policing often proves insufficient for protecting civil rights and civil liberties in the national security context. And even where internal guidelines are ideal, independent checks and safeguards are needed to ensure that limits cannot be rolled back by the very agency governed by them. As more information about specific AI uses is revealed, it will be necessary for Congress to step in for those AI technologies that have the greatest potential to impact rights, codify agency rules that are effective, and establish additional safeguards as necessary. For example, CDT has previously issued a set of key policy recommendations for facial recognition centered on 1) warrants, 2) a serious crime limit, 3) disclosure to arrested individuals, 4) testing and accuracy standards, and 5) limiting the degree of reliance on matches for law enforcement activities.[35] Those rules are critical given the specific risks facial recognition poses, and were crafted to account for how best to protect civil rights and civil liberties while also maximizing efficacy given particular uses of that technology. Congress should work to develop and implement properly tailored rules for other AI technologies that are especially rights-impacting as we obtain greater knowledge on their use.

V. Careful Evaluation of AI Is Key to Defending Against Modern Threats

As Congress evaluates government use of AI in the national security space and proper safeguards, it is also important to consider how understanding and preparing for use of AI is necessary to defend against modern threats to security. This vigilance will be necessary in a variety of spheres.

Congress should rigorously examine use of AI within critical infrastructure. Malicious tampering with AI systems deployed in critical infrastructure could have disastrous implications for national security, especially because the dangerous outputs from such tampered systems might not be readily apparent. These risks are just as present for AI applications in critical infrastructure that are entirely disconnected from security operations (such as an automated system for tracking power usage and distributing energy availability) as those built specifically for it (such as facial recognition systems at airports).[36]

---

[35] See, *Artificial Intelligence and Human Rights: Hearing Before the Sen. Subcomm. on Human Rights and the Law of the Sen. Comm. on the Jud.*, 118th Cong. (2023) (testimony of Alexandra Reeve Givens, President and CEO, Center for Democracy & Technology), https://perma.cc/5ZKF-J97B.

[36] See, Dept. of Homeland Security, *Artificial Intelligence Roadmap 2024*, at 6 (2024), https://perma.cc/Y6KQ-5J9V ("Generating and passing poisoned data into a critical sensor could trigger downstream impacts, such as service disruptions or system shut-offs").

We should also be wary how adversaries might harness AI to augment longstanding attack threats, such as in terms of cybersecurity.[37] Bad actors will use AI to augment the scale of attacks, such as having AI technologies help write and augment software deployed in malicious hacking efforts. AI can also provide new weapons in furtherance of more traditional hacking methods. For example a dedicated spear phishing attack previously conducted via an email or text message could in the future be accompanied by a deep fake voice or video message to increase the odds of deceiving a target. AI itself may prove useful to mitigating these threats — a variety of technological advances have been applied in cybersecurity settings to tip the balance back and forth between attackers and defenders. We should be vigilant in identifying AI-based cybersecurity threats and swift in responding to them, but must also consistently adhere to principles for responsible use of AI, even as a countermeasure to emerging threats. Doing so is the only way to ensure these responses are effective.

Election security is another area where AI technologies may present risks. Generative AI could be used to create convincing fake election records, or produce FOIA requests at a mass scale designed to overwhelm election officials.[38] AI technologies not only expand the range of possible malicious activities, they make misconduct feasible at a larger scale and lower costs. The decentralized nature of our election system adds to the challenge of defending this space. Federal agencies already coordinate information on cybersecurity risks across thousands of election jurisdictions as they emerge through the Election Infrastructure Information Sharing and Analysis Center, provide funding through election security grants, support election officials and administrators, and assist in educating the public about where to find accurate information about elections. Actors in this space should also identify and account for AI-based threats as they emerge. Additionally, while federal agencies' application of AI in the elections space is limited, they should provide oversight and guidance on the use of these tools to state and local election administrators.[39]

Conclusion

While the scope and capabilities of AI technologies may be daunting, executive agencies and Congress should treat it with the same careful consideration as any other powerful machine. Safety, security, and promotion of democratic values can only stem from responsible use. Achieving this requires adherence to principles such as those described above, and Congress has a key role in establishing the oversight and transparency mechanisms that will advance those principles. If we rush to deploy AI quickly rather than carefully, it will harm security and civil liberties alike. But if we establish a strong foundation now for responsible use, we can reap benefits well into the future.

---

[37] As DHS highlights in its recently published AI Roadmap, "The proliferation of accessible AI tools likely will bolster our adversaries' tactics. Cyber actors use AI to develop new tools that allow them to access and compromise more victims and enable larger scale cyber-attacks that are faster, more efficient, and more evasive." *Id.*

[38] See Tim Harper, "CDT Hosts Roundtable on Generative AI and Elections with U.S. Department of State Bureau of Cyberspace and Digital Policy", Center for Democracy & Technology, Mar. 13, 2024, https://perma.cc/5Q9A-J7GJ.

[39] While generative AI has yet to be adopted in any meaningful way by election officials, non-generative AI has been introduced into election administration in recent years. Some election offices have used AI-powered software for administrative purposes including matching mail-in ballot signatures or translating voting materials. See Edgardo Cortés et al, *Safeguards for Using Artificial Intelligence in Election Administration*, Brennan Center for Justice (2023), https://perma.cc/86VR-A82A.