epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

Solicitation of Written Comments by the National Security Commission on Artificial Intelligence

85 Fed. Reg. 32,055

September 30, 2020

By notice published on May 28, 2020, the National Security Commission on Artificial Intelligence ("NSCAI") has requested public comments "to be considered by the Commission in the formation of its final report," currently slated for publication in March 2021.[1] The Electronic Privacy Information Center ("EPIC") submits these comments to the NSCAI (1) to recommend the use of the Universal Guidelines for Artificial Intelligence ("UGAI")[2] and the Organisation for Economic Co-operation and Development AI Principles ("OECD AI Principles")[3] as a basis for U.S. AI policy; (2) to urge the Commission to recommend congressional enactment of government-wide AI safeguards; and (3) to respond to specific recommendations set forth by the Commission in its recent reports.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and human rights issues and to protect privacy,

---

[1] Nat'l Sec. Comm'n Artificial Intelligence, *Solicitation of Written Comments by the National Security Commission on Artificial Intelligence*, 85 Fed. Reg. 32,055 (May 28, 2020) [hereinafter *Solicitation of Written Comments*], https://www.federalregister.gov/documents/2020/05/28/2020-11453/solicitation-of-written-comments-by-the-national-security-commission-on-artificial-intelligence.
[2] The Public Voice, *Universal Guidelines for Artificial Intelligence* (Oct. 23, 2018) [hereinafter *UGAI*], https://thepublicvoice.org/ai-universal-guidelines/.
[3] OECD, *Recommendation of the Council on Artificial Intelligence* (May 21, 2019) [hereinafter *OECD AI Principles*], https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

freedom of expression, and democratic values in the information age.[4] EPIC has a long history of promoting transparency and accountability for the use of automated decision-making systems and has consistently advocated for the adoption of the UGAI.[5] EPIC has litigated cases against the U.S. Department of Justice for documents regarding "risk assessment tools"[6] and against the U.S. Department of Homeland Security for documents about a program designed to assess the likelihood that an individual would commit a crime in the future.[7] In 2018, EPIC joined leading scientific societies in successfully petitioning the U.S. Office of Science and Technology Policy to solicit public input on U.S. Artificial Intelligence Policy.[8] EPIC also submitted comments urging the National Science Foundation to adopt the UGAI and to promote and enforce the UGAI across the funding, research, and deployment of AI systems.[9] EPIC has published two editions of the *AI Policy Sourcebook*, the first comprehensive reference book on AI policy.[10]

I. EPIC urges the NSCAI to rely on the Universal Guidelines for Artificial Intelligence and the OECD AI Principles as a baseline for AI regulation.

EPIC supports the NSCAI's stated goals of encouraging international cooperation on the safe use of AI; ensuring robust ethical protections at every stage of AI design and deployment; and

---

[4] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.
[5] *See, e.g.*, Comments of EPIC, *Intellectual Property Protection for Artificial Intelligence Innovation*, U.S. Patent and Trademark Office (Jan. 10, 2020), https://epic.org/apa/comments/EPIC-USPTO-Jan2020.pdf; Comments of EPIC, *HUD's Implementation of the Fair Housing Act's Disparate Impact Standard*, Department of Housing and Urban Development (Oct. 18, 2019), https://epic.org/apa/comments/EPIC-HUD-Oct2019.pdf; Testimony of EPIC to the Mass. Joint Comm. on the Judiciary (Oct. 22, 2019), https://epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf; Statement of EPIC, *Industries of the Future*, S. Comm. on Commerce, Sci. & Transp. (Jan. 15, 2020), https://epic.org/testimony/congress/EPIC-SCOM-AI-Jan2020.pdf; Comments of EPIC, *Request for Information: Big Data and the Future of Privacy*, Office of Sci. and Tech. Policy (Apr. 4, 2014).
[6] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)*, https://epic.org/foia/doj/criminal-justice-algorithms/ (2019).
[7] *See id.*; EPIC, *EPIC v. DHS (FAST Program)*, https://epic.org/foia/dhs/fast/ (2018).
[8] EPIC, *Petition to OSTP for Request for Information on Artificial Intelligence Policy* (July 4, 2018), https://epic.org/privacy/ai/OSTP-AI-Petition.pdf.
[9] EPIC, *Request for Information on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan* Oct. 26, 2018), https://epic.org/apa/comments/EPIC-Comments-NSF-AI-Strategic-Plan-2018.pdf.
[10] EPIC, *EPIC AI Policy Sourcebook 2020* (2020), https://epic.org/bookstore/ai2020/.

protecting individuals against the harms that AI systems may cause. EPIC urges the Commission to rely on the UGAI and the OECD AI Principles as a framework for achieving these objectives.

The Universal Guidelines for Artificial Intelligence, a set of AI principles based on the protection of human rights, were set out at the 2018 Public Voice meeting in Brussels, Belgium.[11] The Universal Guidelines have been endorsed by more than 250 experts and 60 organizations in 40 countries.[12] The UGAI consist of twelve principles:

1. **Right to Transparency.** All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome.
2. **Right to Human Determination.** All individuals have the right to a final determination made by a person.
3. **Identification Obligation.** The institution responsible for an AI system must be made known to the public.
4. **Fairness Obligation.** Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.
5. **Assessment and Accountability Obligation.** An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.
6. **Accuracy, Reliability, and Validity Obligations.** Institutions must ensure the accuracy, reliability, and validity of decisions.
7. **Data Quality Obligation.** Institutions must establish data provenance, and assure quality and relevance for the data input into algorithms.
8. **Public Safety Obligation.** Institutions must assess the public safety risks that arise from the deployment of AI systems that direct or control physical devices, and implement safety controls.
9. **Cybersecurity Obligation.** Institutions must secure AI systems against cybersecurity threats.
10. **Prohibition on Secret Profiling.** No institution shall establish or maintain a secret profiling system.
11. **Prohibition on Unitary Scoring.** No national government shall establish or maintain a general-purpose score on its citizens or residents.
12. **Termination Obligation**. An institution that has established an AI system has an affirmative obligation to terminate the system if human control of the system is no longer possible. [13]

[11] *UGAI*, *supra* note 2.
[12] The Public Voice, *Universal Guidelines for Artificial Intelligence: Endorsement* (2020), https://thepublicvoice.org/AI-universal-guidelines/endorsement/.
[13] *UGAI*, *supra* note 2.

The OECD AI Principles were adopted in 2019 and endorsed by 42 countries—including the United States and the G20 nations. The OECD AI Principles establish international standards for AI use:

1. **Inclusive growth, sustainable development and well-being.** AI should benefit people and the planet.
2. **Human-centered values and fairness.** AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards—for example, enabling human intervention when necessary—to ensure a fair and just society.
3. **Transparency and explainability.** There should be transparency and a responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
4. **Robustness, security and safety.** AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.
5. **Accountability.** Organizations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.[14]

In many respects, the consensus principles and lines of effort set out by the NSCAI align with the UGAI and the OECD AI Principles. For example, the Commission agrees that "[e]thical and trustworthy AI is a strategic and operational necessity"; that "reliability, robustness, auditability, explainability, and fairness" are essential for responsible AI deployment; that "design and deployment of AI . . . must align with America's democratic values and institutional values"; and that "ethical AI systems for national security will need to preserve individual rights and liberties as protected by law," including "humanitarian law and human rights."[15] Consistent with the spirit of the OECD AI Principles, the Commission also urges the U.S. to "lead in establishing a positive agenda for cooperation with all nations on AI advances that promise to benefit humanity."[16]

[14] *Recommendation of the Council on Artificial Intelligence*, OECD (May 21, 2019) [hereinafter *OECD AI Principles*], https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[15] *Solicitation of Written Comments*, *supra* note 1.
[16] *Id.*

Still, the Commission should do more to operationalize the UGAI and the OECD AI Principles. For example, the NSCAI should recommend that Congress, the Office of Management and Budget, and federal agencies impose and uphold rigorous procurement and development standards for the use of AI. Ethical design is an indispensable component of trustworthy AI. Yet the Commission's support for rapid adoption of commercially available AI tools[17] is in tension with the principle of designing AI systems with ethics in mind from the earliest phase.

Further, it is not enough to assert that trustworthy AI is an operational necessity—or to insist that it conform with "American values" and "the rule of law"—unless the Commission also calls for specific, enforceable legislation and regulations to ensure that AI safeguards are observed. EPIC urges the Commission to endorse binding legal obligations on federal agencies consistent with the UGAI, including the requirement that "the factors, logic and techniques" of an AI system be accessible to anyone whom the system affects;[18] the requirement that "the institution responsible for an AI system must be made known to the public";[19] the requirement that "an AI system . . . be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks"[20]; and the prohibitions on secret profiling systems and general-purpose social scoring.[21]

II. The NSCAI should urge Congress to establish government-wide baseline principles for the use of AI.

As the NSCAI has acknowledged, it is essential that any AI system developed or used by a federal agency be "responsible, trusted, and ethical[.]"[22] For this reason, the Commission has

[17] Nat'l Sec. Comm'n Artificial Intelligence, *Second Quarter Recommendations* 93 (July 2020) [hereinafter *Second Quarter Recommendations*], https://drive.google.com/file/d/1hgiA38FcyFcVQOJhsycz0Ami4Q6VLVEU/view.
[18] *UGAI*, *supra* note 2.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Second Quarter Recommendations*, *supra* note 17, at vii.

correctly called for an "intentional, government-wide, coordinated effort"[23] to establish "practical guidance for implementing commonly agreed upon AI principles and a more comprehensive strategy to develop and field AI responsibly."[24] An uneven or haphazard implementation of AI principles will not do: as the Commission has underscored, there must be "inter-agency consistency in prioritizing the recommended practices[.]"[25]

EPIC fully agrees. That is why the NSCAI must advise Congress, as the nation's highest policymaking authority, to establish government-wide principles and safeguards for the use and development of AI. There is no entity better situated than Congress to set baseline limits on the use of AI, and there is no tool more powerful than a federal statute to ensure agency compliance. Anything less will fail to achieve the coordination, consistency, and comprehensive federal strategy that the Commission believes necessary for responsible AI deployment.

It is unfortunate, then, that the NSCAI has failed to urge Congress to enact baseline AI principles. In most areas of its work, the Commission has made ambitious, detailed recommendations for congressional action on AI. The Commission's first and second quarter reports contain dozens of legislative proposals, including the establishment of the National Reserve Digital Corps and United States Digital Service Academy,[26] the appropriation of hundreds of millions of dollars for AI initiatives,[27] the creation of tax credits for private sector AI development,[28] and the

[23] *Id.* at 97.
[24] *Id.* at 93.
[25] *Id.*
[26] *Id.* at 34.
[27] *Id.* at 184.
[28] *Id.* at 66.

enactment of comprehensive foreign relations reauthorization legislation.[29] The Commission has even offered up 65 pages of draft statutory language to facilitate speedy action by Congress.[30]

Yet when it comes to ensuring "responsible, trusted, and ethical" AI, the NSCAI's advice to Congress is scant. Congress's recommended role is limited to (1) requiring federal agencies to share their AI training programs with state, local, and tribal governments;[31] (2) establishing a "board of interdisciplinary experts qualified to speak on emerging considerations for ethical and responsible AI";[32] (3) mandating a federal strategy for AI documentation;[33] (4) requiring agencies to conduct self-assessments of their own access to AI experts;[34] and (5) "asking critical questions of agency leadership and those responsible for AI systems."[35] These are all sensible recommendations—but far short of the leading role that Congress must play in ensuring that U.S. deployment of AI is responsible, ethical, and consistent with constitutional and human rights.

Nor has the Commission adequately explained its failure to recommend statutory AI safeguards. During the NSCAI's July 20, 2020 plenary meeting, Commissioner Eric Horvitz, Chief Scientific Officer of Microsoft, implied that it was too soon for Congress to weigh in on the ethics of AI:

> We're still learning a lot about what it means to take principles like fairness, inclusiveness, transparency, and other what we would call 'principles of ethics' into the world. . . . The idea of saying there's one thing called ethical principles, and we demand Congress do legislation around this and coordinate, I think is a challenging one.[36]

---

[29] *Id.* at 92.
[30] *See id.* at 164–83; Nat'l Sec. Comm'n Artificial Intelligence, *First Quarter Recommendations* 79–123 (March 2020) [hereinafter *First Quarter Recommendations*], https://drive.google.com/file/d/1wkPh8Gb5drBrKBg6OhGu5oNaTEERbKss/view.
[31] *Id.* at 70.
[32] *Id.* at 71.
[33] *Id.* at 73.
[34] *Id.* at 74.
[35] *Second Quarter Recommendations*, *supra* note 17, at 155.
[36] NSCAI, *National Security Commission on AI, Public Meeting*, YouTube (July 20, 2020), https://www.youtube.com/watch?v=G4ynnACMnQ8.

Commissioner Mignon Clyburn, former member and acting chairwoman of the Federal Communications Commission, added that the responsibility for AI regulation should fall to "a number of complementary players":

> [W]hen you speak of a legislative or a congressional solution, that is but a snapshot in time. And so, that is why a blended approach and a number of complementary players are needed. Some are more nimble and can act more in real time, and others—like I said—legislative bodies, laws can also be static even though the application may not be. And that's where the other players come in.[37]

But neither of these concerns justifies sidelining Congress from the vital project of regulating government AI use.

First, it is the Commission's statutory obligation to offer Congress advice concerning the "ethical considerations" of AI, including "recommendations to more effectively organize the Federal Government."[38] The Commission has already urged Congress to make enormous investments in U.S. AI development and to rapidly accelerate the federal government's adoption of AI. Having done so, it irresponsible of the Commission not to propose corresponding legislative safeguards on AI deployment. AI systems—particularly those used in defense and national security settings—present profound risks to privacy, safety, and human rights. Unless express, binding limits on the use of AI are established *now*, the technology will quickly outpace our collective ability to regulate it. The Commission cannot simply kick the can down the road, particularly when governments, civil society, and private sector actors have already laid extensive groundwork for the regulation of AI.[39]

Second, congressional enactment of AI principles would be the first word, not the last or the only word, on the responsible use of AI. Each federal agency would still enjoy significant control

[37] *Id.*
[38] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1051, 132 Stat. 1636 (2018).
[39] *See, e.g.*, *UGAI*, *supra* note 2; *OECD AI Principles*, *supra* note 3.

over how to implement baseline AI standards—consistent with governing law—through publicly accountable notice-and-comment rulemaking. And both Congress and federal agencies would retain their respective power to modify or add to AI safeguards as circumstances require. Concerns about "nimble[ness]"[40] and "flexibility"[41] need not interfere with establishing a common, robust, and legally enforceable set of baseline AI principles.

In sum, the NSCAI must urge Congress to establish fundamental AI safeguards that will apply government-wide. As explained above, the OECD AI Principles and UGAI offer the Commission a template for a detailed legislative proposal to Congress.

III. The NSCAI should recommend a prohibition on the procurement of commercially avaible AI systems unless a system is necessary for a valid public purpose, thoroughly vetted, and backed by robust accountability measures.

The NSCAI has characterized U.S. global leadership in AI development as a top priority.[42] EPIC agrees that the U.S. should set an example for the world by developing safe, productive, purpose-driven AI. However, EPIC warns the Commission that incentivizing the adoption of commercial software tools and "moderniz[ing]" solely to gain a competitive edge will undermine the U.S.'s principled leadership on AI.[43]

The Commission contends that the rapid adoption of commercially available AI is essential to achieving U.S. leadership in the field.[44] But before the federal government procures any AI system, it is crucial that there be a specified public purpose for the adoption of the system; a fulsome and transparent process through which alternative systems and approaches are weighed; and robust accountability measures, including an opportunity for individuals unfairly harmed by the system to

[40] *National Security Commission on AI, Public Meeting*, *supra* note 36.
[41] *Second Quarter Recommendations*, *supra* note 17, at 94.
[42] *E.g.*, *Solicitation of Written Comments, supra* note 1 (Consensus Principles 1, 2; Line of Effort 2; Line of Effort 3).
[43] *Second Quarter Recommendations*, *supra* note 17, at 10.
[44] *Id.*

obtain redress. These safeguards are particularly important in defense and national security contexts, where privacy, safety, and human rights are often at greatest risk.

Although the adoption of AI by federal government is growing—a February 2020 report found that nearly half of the 142 federal agencies studied had "experimented with AI and related machine learning tools"[45]—many of the AI tools procured by government agencies have proven to be deeply flawed. For example, in the criminal justice system, the deployment of AI and other algorithmic decision-making tools tends to exacerbate discriminatory policing patterns that already disadvantage minorities. A 2019 National Institute of Standards and Technology ("NIST") study of facial recognition tools—which are typically "AI-based"[46]—found that the systems were up to 100 times more likely to return a false positive for a non-white person than for a white person.[47] Specifically, NIST found that "for one-to-many matching, the team saw higher rates of false positives for African American females," a finding that is "particularly important because the consequences could include false accusations."[48] A separate study by Stanford University and MIT, which looked at three widely deployed commercial facial recognition tools, found an error rate of 34.7% for dark-skinned women compared to an error rate of 0.8% for light-skinned men.[49] A review of Rekognition—an Amazon-owned facial recognition system marketed to law enforcement—revealed indications of racial bias and found that the system misidentified 28 members of U.S.

[45] David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, & Mariano-Florentino Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* 6 (Feb. 2020) https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.
[46] Nat'l Inst. Standards & Tech., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 14 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[47] Nat'l Inst. Standards & Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
[48] *Id*.
[49] Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News (Feb. 11, 2018), http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

Congress as convicted criminals.[50] Similarly, AI and algorithmic decision-making tools used in pretrial dispositions, sentencing, and prison settings often yield inaccurate or biased results that perpetuate existing inequalities.[51]

Because these AI systems and algorithms are ordinarily unaccountable and opaque, they present exceptional risks to fundamental rights. For this reason, EPIC urges the NSCAI to recommend that any AI system adopted by a federal agency be supported by a valid public purpose, thoroughly vetted, and backed by accountability measures that allow a person unduly harmed by the system to obtain redress.

IV. The NSCAI should more clearly distinguish between recommendations intended for national security and defense contexts and those that are intended to apply more broadly.

The National Defense Authorization Act for 2019 charges the NSCAI with studying "ethical considerations related to artificial intelligence and machine learning as it will be used for future applications *related to national security and defense*."[52] However, at several points the Commission has made recommendations concerning the use of AI by state, local, and tribal law enforcement agencies;[53] has strayed into discussions of U.S. diplomacy and trade policy;[54] and has even gone out of its way to attack the European Union's General Data Protection Regulation.[55]

---

[50] Russell Brandom, *Amazon's facial recognition matched 28 members of Congress to criminal mugshots*, The Verge (July 26, 2018), https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

[51] *See, e.g.*, EPIC, *Algorithms in the Criminal Justice System: Pre-Trial Risk Assessment Tools* https://epic.org/algorithmic-transparency/crim-justice/; Melissa Hamilton, *The Biased Algorithm: Evidence of Disparate Impact on Hispanics*, 56 Am. Crim L. Rev. 1553 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251763; Megan T. Stevenson & Christopher Slobogin, *Algorithmic Risk Assessments and the Double-Edged Sword of Youth*, 96 Wash. U.L. Rev. 681 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3225350; Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[52] § 1051(b)(2)(G) (emphasis added).

[53] *First Quarter Recommendations*, *supra* note 30, at 70.

[54] *Id.* at 54.

[55] Nat'l Sec. Comm'n Artificial Intelligence, *Interim Report* 90–91 (Nov. 2019), https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view (footnote 179).

EPIC is not opposed to the Commission opining on AI issues outside of the national security and defense context; indeed, EPIC believes that the Commission should call on Congress to establish baseline, government-wide safeguards for the use of AI. Nevertheless, EPIC urges the NSCAI to clearly identify the scope and substantive applicability of its recommendations. Although many AI safeguards—like those set forth in the UGAI and the OECD AI Principles—should be universally observed, the use of AI in domestic law enforcement and commercial contexts presents unique concerns and considerations. Accordingly, the Commission should clearly state which of its recommendations apply to defense and national security settings and which of its recommendations are intended to reach more broadly.

V. Conclusion

As set forth above, EPIC urges the NSCAI to rely on the Universal Guidelines for AI and the OECD AI Principles as a baseline for AI regulation; to recommend that Congress enact government-wide AI safeguards; to ensure strict limitations on government procurement of commercially produced AI systems; and to clearly convey the substantive reach of each of its recommendations.

Respectfully submitted,

/s/ John Davisson
John Davisson
EPIC Senior Counsel

/s/ Ben Winters
Ben Winters
EPIC Equal Justice Works Fellow