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 INSTITUTE OF STANDARDS AND TECHNOLOGY

Request for Comment on Study to Advance a More Productive Tech Economy

86 Fed. Reg. 66,287

February 15, 2022

By notice published on November 22, 2021, the National Institute of Standards and Technology ("NIST") has requested information "on the public and private sector marketplace trends, supply chain risks, legislative, policy, and the future investment needs of eight emerging technology areas."[1] In particular, NIST seeks "comments to help identify, understand, refine, and guide the development of the current and future state of technology" in the areas of "Artificial Intelligence, Internet of Things in Manufacturing, Quantum Computing, Blockchain Technology, New and Advanced Materials, Unmanned Delivery Services, Internet of Things, and Three-dimensional Printing."[2]

The Electronic Privacy Information Center ("EPIC") submits these comments to share recommendations and expertise with NIST. EPIC is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values.[3] EPIC has a long

[1] Study to Advance a More Productive Tech Economy, 86 Fed. Reg. 66,287 (Nov. 22, 2021),
[2] *Id.*
[3] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.

history of promoting transparency and accountability for information technology.[4] EPIC has advocated for transparency and accountability internationally in connection with the use of AI systems.[5] EPIC has litigated cases against the U.S. Department of Justice to compel production of documents regarding "evidence-based risk assessment tools"[6] and against the U.S. Department of Homeland Security to produce documents about a program purported to assess the probability of whether an individual committed a crime.[7] In 2018, EPIC and leading scientific societies petitioned the U.S. Office of Science and Technology Policy to solicit public input on U.S. Artificial Intelligence Policy.[8] EPIC submitted comments urging the National Science Foundation to adopt the Universal Guidelines for Artificial Intelligence ("UGAI") and to promote and enforce the UGAI across funding, research, and deployment of U.S. AI systems.[9] EPIC has also submitted comments to the National Security Commission on Artificial Intelligence, the U.S. Office of Science and Technology Policy, the European Commission, and the U.S. Office of Management and Budget among many others urging the adoption of AI safeguards that meaningfully protect individuals.[10]

---

[4] EPIC, *AI & Human Rights* (2022), https://epic.org/issues/ai/; EPIC, *AI in the Criminal Justice System* (2022), https://epic.org/issues/ai/ai-in-the-criminal-justice-system/; Comments of EPIC, *In re Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics*, Federal Trade Commission (Aug. 20, 2018), https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-20-2018.pdf; Comments of EPIC, *In re Developing UNESCO's Internet Universality Indicators: Help UNESCO Assess and Improve the Internet*, United Nations Educ., Sci. & Cultural Org. (Mar. 15, 2018), https://epic.org/wp-content/uploads/apa/comments/EPIC_UNESCO_Internet_Universality_Comment.pdf.

[5] EPIC, AI & Human Rights, *supra* note 4.

[6] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)* (2020), https://epic.org/foia/doj/criminal-justice-algorithms/.

[7] *See id.*; EPIC, *EPIC v. AI Commission* (2021), https://epic.org/documents/epic-v-ai-commission/; *EPIC v. DHS (FAST Program)* (2015), https://epic.org/foia/dhs/fast/.

[8] Petition from EPIC et al. to OSTP (July 4, 2018), https://epic.org/privacy/ai/OSTP-AI-Petition.pdf.

[9] Comments of EPIC, Request for Information on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan, 83 Fed. Reg. 48,655 (Oct. 26, 2018), https://epic.org/apa/comments/EPIC-Comments-NSF-AI-Strategic-Plan-2018.pdf.

[10] Comments of EPIC, *EPIC Comments to OSTP on Public and Private Sector Uses of Biometric Technologies*, Office of Science and Technology Policy (Jan. 15, 2022); Comments of EPIC, *Artificial Intelligence Risk Management Framework*, National Institute of Standards and Technology (Aug. 18, 2021), https://epic.org/documents/regarding-the-artificial-intelligence-risk-management-framework/; Comments of

EPIC urges NIST to advocate for rules guiding the development of artificial intelligence like the Universal Guidelines for Artificial Intelligence, to recommend that Congress remedy the discrepancy between funding for AI development and AI oversight, recognize that privacy and data protection drive innovation, and call for privacy laws to address the expansion of the uncrewed drone industry, including drone delivery.

I. NIST's recommendations should reflect a clear, comprehensive, and protective set of guidelines such as the Universal Guidelines for Artificial Intelligence.

Although there have been many AI principles set forth by industry, academia, civil society, and governments, EPIC recommends that NIST use the Universal Guidelines for Artificial Intelligence ("UGAI") as baseline framework for the responsible governance of AI. The UGAI, based on the protection of human rights, were set out at the 2018 Public Voice meeting in Brussels, Belgium.[11] The UGAI have been endorsed by more than 250 experts and 60 organizations in 40 countries.[12] The twelve guidelines are:

1. Right to Transparency.
2. Right to Human Determination.

EPIC, *Request for Information (RFI) on an Implementation Plan for a National Artificial Intelligence Research Resource*, Office of Science and Technology Policy and National Science Foundation (Oct. 1, 2021); Comments of EPIC, *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, Comptroller Of The Currency; Federal Reserve System; Federal Deposit Insurance Corporation; Consumer Financial Protection Bureau; National Credit Union Administration, (July 1, 2021), https://archive.epic.org/apa/comments/EPIC-Financial-Agencies-AI-July2021.pdf; https://epic.org/documents/epic-comments-to-ostp-on-public-and-private-sector-uses-of-biometric-technologies/; Comments of EPIC, Solicitation of Written Comments by the National Security Commission on Artificial Intelligence, 85 Fed. Reg. 32,055 (Sep. 30, 2020), https://epic.org/apa/comments/EPIC-comments-to-NSCAI-093020.pdf; Comments of EPIC, Request for Comments on a Draft Memorandum to the Heads of Executive Departments and Agencies, "Guidance for Regulation of Artificial Intelligence Applications," 85 Fed. Reg. 1,825 (Mar. 13, 2020), https://epic.org/apa/comments/EPIC-OMB-AI-MAR2020.pdf; Comments of EPIC, *Request for Feedback in Parallel with the White Paper on Fundamental Rights*, European Commission Fundamental Rights Policy Unit (May 29, 2020), https://epic.org/apa/comments/EPIC-EU-Commission-AI-Comments-May2020.pdf; Comments of EPIC, *Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence*, European Commission (Sep. 10, 2020), https://epic.org/apa/comments/EPIC-EU-Commission-AI-Sep2020.pdf.

[11] *Universal Guidelines for Artificial Intelligence*, The Public Voice (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/.

[12] *Id.*

3. Identification Obligation.
4. Fairness Obligation.
5. Assessment and Accountability Obligation.
6. Accuracy, Reliability, and Validity Obligations.
7. Data Quality Obligation.
8. Public Safety Obligation.
9. Cybersecurity Obligation.
10. Prohibition on Secret Profiling.
11. Prohibition on Unitary Scoring.
12. Termination Obligation.[13]

II. NIST should urge Congress to balance the funding of AI development and research with the establishment and funding of meaningful oversight mechanisms.

To date, Congress has directed a disproportionate amount of federal funding to the development and deployment of AI and to public-private AI partnerships, while comparatively little funding has been set aside for necessary oversight of AI. This is apparent in the annual National Defense Authorization Act ("NDAA"); in recommendations from the National Security Commission on Artificial Intelligence; and in the development of the National AI Research Resource.[14]

Although EPIC shares in the goal of making the United States a leader in the responsible use of AI, current funding and support streams do not reflect a serious commitment to achieving that goal. One example that illustrates this dynamic is the NDAA for fiscal year 2022, which dedicates over $3 billion to research, capacity building, and the development of emerging technologies. Meanwhile, Congress has failed to institute meaningful oversight or regulation of AI despite overwhelming evidence of the inaccuracy, bias, and human rights risks that plague many AI systems. The strongest government-wide transparency effort was established through an Executive

[13] *Id.*
[14] *See, e.g.*, *National Defense Authorization Act for Fiscal Year 2022*, https://www.armed-services.senate.gov/imo/media/doc/FY22%20NDAA%20Executive%20Summary.pdf; National Security Commission on Artificial Intelligence, *Final Report* (Mar. 1, 2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

Order, but with no additional resources or congressional mandate, agencies' obligations under that Order have gone unfulfilled.[15]

NIST should recommend that Congress invest substantial resources in the development and implementation of third-party, independent audits and impact assessments for AI in both the public and private sectors. Funds should also be appropriated to establish and enforce minimum data governance and minimization requirements; to ensure that agencies adequately evaluate and publish information about the AI systems they procure and develop; and to determine which AI tools are discriminatory, inaccurate, or otherwise fundamentally incompatible with the protection of human and civil rights.

III. The United States urgently needs a uniform baseline AI law that imposes transparency, accountability, and appropriate red lines.

A regulatory approach to AI that focuses almost exclusively on data sharing, AI research and development, and public-private partnerships is a threat to privacy and human rights. As EPIC warned the NSCAI in September 2020, "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.[16]" A different strategy is required.

NIST should urge Congress to establish baseline legal safeguards for both government and commercial use of AI. EPIC recommends that NIST and Congress rely on the UGAI as a baseline framework for regulating AI, and would further recommend that Congress:

- Establish a moratorium or ban on particularly harmful, inaccurate, and unaccountable AI systems (e.g., biometric and emotional analysis);
- Require *public and easily accessible* documentation of AI systems that will enable individuals to understand and identify the origin and operator of each system;

[15] Exec. Order 13,960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (Dec. 8, 2020), https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.
[16] NSCAI *Second Quarter Recommendations*, *supra* note 17, at 10, https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI-Q2-Memo_20200722.pdf.

- Impose purpose specification and use limitation requirements on AI systems to mitigate mission creep;
- Provide an opportunity for individuals unfairly harmed by AI systems to obtain redress;
- Limit the collection of personal information by AI systems without express, informed consent; and
- Institute a ban on profiling.

The widespread collection, use, and retention of personal information by AI systems and the resulting risk of harm also underscores the need for Congress to enact comprehensive baseline data protection legislation.

IV. Encouraging privacy-centric innovation will spur economic growth, promote competition, and benefit consumers.

NIST's final report should emphasize the role that data protection and privacy can play in "foster[ing] economic growth and competitiveness" and "promot[ing] U.S. innovation and industrial competitiveness."[17] Too often, legal safeguards on the collection and use of personal information are assumed to be at odds with innovation and economic growth. But this view of privacy as merely a regulatory burden ignores the ways in which data protection will benefit consumers, strengthen market competition, and lead to the development of better and more popular products and services. Time and again, studies have found that the American public cares strongly about protecting personal data from commercial exploitation and will opt for credible privacy-protective alternatives when they are available.[18] For example, when Apple recently gave iOS users the power to easily

[17] Study to Advance a More Productive Tech Economy, 86 Fed. Reg. 66,287.
[18] *See, e.g.*, Cisco Secure, *Building Consumer Confidence Through Transparency and Control* (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (finding that 86% of respondents "care about data privacy" and "want more control," while 79% are "willing to spend time and money to protect data" and "pay more"); Sam Sabin, *States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data*, Morning Consult (Apr. 27, 2021), https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/ (finding that 83% of voters believe Congress should enact privacy legislation); Brooke Auxier et al., Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (finding that 75% of respondents believe there should be new regulations of what companies may do with personal data).

block advertisers from tracking them across multiple apps, 96% of users opted out of such tracking.[19] Establishing a robust data protection framework will spur producers and developers of data-driven products and services to tap into consumer desire for privacy protection and to build better and less extractive technologies. Requiring American companies to lead the way in privacy innovation will also strengthen their competitive edge and position U.S. technology firms for continued growth in a privacy-conscious economy.

V. Strong drone privacy laws will strengthen American firms' position domestically and abroad while building consumer trust in new technologies.

NIST's final report should draw attention to the current lack of privacy regulations for uncrewed aircraft, the substantial privacy threats that unregulated drone deliveries may pose, and the urgent need for Congress to act to set baseline privacy rules for uncrewed delivery and uncrewed vehicles generally.

EPIC was the first privacy organization to identify and oppose the threat of drone surveillance. Today EPIC is engaged on a variety of fronts to shape drone policy, to prevent and roll back aerial surveillance programs, and to address the growing dangers of corporate drone use. EPIC regularly comments on proposed rulemakings by the Federal Aviation Administration and FCC that would regulate or expand the use of drones. EPIC also advocates for foregrounding privacy protections in the rollout of drones by serving on government advisory boards.

In the past EPIC has fought for transparency in government-industry drone policy planning projects[20] and has used the Freedom of Information Act to uncover information about government

[19] Samuel Axon, *96% of US Users Opt Out of App Tracking in iOS 14.5, Analytics Find*, Ars Technica (May 7, 2021), https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/.

[20] *See EPIC v. Drone Advisory Committee*, https://epic.org/documents/epic-v-drone-advisory-committee/ (detailing EPIC's suit to enforce the transparency obligations of a body created by the Federal Aviation Administration to study and make recommendations on U.S. drone policy).

use of drones.[21] EPIC was one of the first organizations to call for a requirement that drones broadcast identifying information and spent years urging the FAA to implement one.[22] The FAA is now in the process of implementing a remote ID requirement, and EPIC continues to push the FAA to enforce that requirement in a privacy-protective manner. The long and arduous process to promulge simple safety regulations to require a remote identifier for drones demonstrates that the government needs to act now to put in place privacy protections for the use of drones.

However, the FAA has repeatedly disclaimed its authority to specifically address drone privacy through the rulemaking process.[23] EPIC first filed a petition for rulemaking with the FAA in 2012, joined by a coalition of over 100 other privacy and civil liberties groups.[24] EPIC twice filed suit to force the FAA to meet its obligations and conduct a drone privacy rulemaking, but both suits were ultimately unsuccessful.[25]

NIST should urge Congress to pass legislation setting baseline privacy rules for uncrewed drone deliveries and directing the FAA to implement further privacy protections for uncrewed aerial systems. These systems pose significant privacy risks, as they are equipped with cameras and other remote sensors. Deploying a fleet of unmanned delivery drones in public areas could result in continuous aerial surveillance that would be unacceptable to the public, and unconstitutional if done by the government.

---

[21] *See, e.g.*, *EPIC v. DHS (Drone Policies)* (2018), https://archive.epic.org/foia/dhs_2/epic_v_dhs_drone_policies.html (detailing EPIC's successful lawsuit to obtain documents from the Department of Homeland Security on the policies governing the agency's use of drones and information obtained from drones).
[22] *See, e.g.*, Comments of EPIC to the Department of Transportation and FAA on Clarification of the Applicability of Aircraft Registration Requirements for Unmanned Aircraft Systems (UAS) (Nov. 12, 2015), https://epic.org/wp-content/uploads/apa/comments/EPIC-FAA-Drone-Reg-Comments.pdf.
[23] *See EPIC v. FAA (Drone Privacy Rulemaking)*, https://epic.org/documents/epic-v-faa/.
[24] EPIC, Petition for Drone Privacy Rulemaking (Feb. 24, 2012), https://epic.org/wp-content/uploads/apa/lawsuit/EPIC-FAA-Drone-Petition-March-8-2012.pdf.
[25] *See EPIC v. FAA (Drone Privacy Rulemaking)*, https://epic.org/documents/epic-v-faa/.

In *Leaders of the Beautiful Struggle v. Baltimore Police Dept*., the Fourth Circuit recently ruled that near-continuous use of spy planes to record detailed video of 32 square miles of Baltimore was a violation of the Fourth Amendment because it "enables police to deduce from the whole of individuals' movements."[26] The type of comprehensive aerial surveillance at issue in *Leaders of the Beautiful Struggle* could also occur through a drone delivery system or other commercial drone fleet implemented without sufficient safeguards. A drone fleet with cameras recording every detail of their flights would create a comprehensive and persistent record of public spaces, including individuals' locations and movements.

Congress should enact rules for both industry and the government to ensure that drones and drone fleets do not infringe on privacy rights. Such protections should include:

- A drone ID requirement to broadcast the identity and location of each drone along with details of the drone's purpose, technical capabilities, and the government or commercial operator (if applicable);
- A prohibition against generalized aerial surveillance by the government or government contractors;
- A warrant requirement for government drone surveillance;
- Restrictions on commercial drone data collection; and
- Transparency requirements for government and commercial operators.

Congress can also look to the comprehensive drone regulations established in the European Union.[27] Enacting similar rules in the U.S. would help position American firms to comply with drone rules in two markets. Strong privacy laws governing the use of drones and commercial drone fleets would also allow American businesses to differentiate themselves from competitors globally and set them up to earn consumer trust domestically.

[26] 2 F.4th 330 (4th Cir. 2021) (en banc), https://epic.org/wp-content/uploads/privacy/Leaders-of-a-Beautiful-Struggle-v-BPD-en-banc-opinion-062421.pdf.
[27] Commission Delegated Regulation (EU) 2019/945, on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (Mar. 12, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN.

VI. Conclusion.

For the reasons above, NIST should ensure that its final report pursuant to section 15 of the Consolidated Appropriations Act endorses clear, comprehensive, and robust AI safeguards; urges Congress to strike a balance between the funding of AI research and the establishment of AI oversight mechanisms; calls for a uniform baseline AI law that will ensure transparency, accountability, and appropriate red lines; emphasizes the role that data protection can play in fostering innovation, competition, and economic growth; and calls for the enactment of baseline privacy rules for uncrewed aircraft. EPIC thanks NIST for its attention to these issues and for taking the time to consider EPIC's recommendations.

Sincerely,

/s/ John Davisson
John Davisson
EPIC Director of Litigation
& Senior Counsel

/s/ Ben Winters
Ben Winters
EPIC Counsel

/s/ Jake Wiener
Jake Wiener
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)