epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL SCIENCE FOUNDATION

Request for Information on Federal Video and Image Analytics
Research and Development Action Plan

87 Fed. Reg. 42,212

September 2, 2022

By notice published on July 14, 2022, the Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO) and National Science Foundation have requested information to update the 2020 Federal Video and Image Analytics (VIA) Research and Development (R&D) Action Plan (VIA R&D Action Plan). NITRD NCO seeks comments on VIA R&D Action Plan's six strategic goals and objectives.[1] In particular, the RFI requests input on revisions to the Action Plan that would "reflect changes in technology and the socio-technical environment over the past four years."[2]

The Electronic Privacy Information Center (EPIC) submits these comments to share recommendations and expertise with NITRD NCO. 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

---

[1] National Science Foundation, *Request for Information on Federal Video and Image Analytics Research and Development Plan*, 87 Fed. Reg. 42,212 (July 14, 2022) [hereinafter *RFI*].
[2] *Id*.
[3] EPIC, *About Us* (2022), https://epic.org/about/.

has a long history of promoting transparency and accountability for information technology.[4] In particular, EPIC has advocated for transparency and accountability in connection with the use of AI systems.[5] 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.[6] EPIC has 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.[7] 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.[8]

---

[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] Petition from EPIC et al. to OSTP (July 4, 2018), https://epic.org/privacy/ai/OSTP-AI-Petition.pdf.
[7] 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.
[8] 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, *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 (Sept. 30, 2020),

EPIC urges NITRD NCO to center privacy and human rights in the revised VIA R&D Action Plan. In particular, the updated Action Plan should include a seventh strategic goal of instituting privacy and human rights safeguards for federal R&D involving VIA. EPIC supports the continuing development of a coordinated federal strategy for VIA R&D, but the uniformity imposed across agencies must include a robust privacy and human rights framework.

I.   The VIA R&D Action Plan's strategic goals and objectives should be expanded to include a goal to protect privacy and human rights.

Because the Action Plan dictates VIA R&D principles across many agencies and partners, NITRD NCO has a responsibility to include as a strategic goal the protection of privacy and human rights. Federal engagement in the VIA R&D Action Plan represents a widespread coalition composed of "researchers from 30 government organizations spanning nearly all Federal agencies[.]"[9] The vision of the 2020 VIA R&D Action Plan was to "foster strategic R&D activities across Federal agencies related to VIA technologies that support the health, safety, prosperity and security of the Nation."[10] However, despite the broad reach and impact of the Action Plan and the stated intention to foster safe innovation, the Action Plan did not mention privacy or human rights risks and concerns related to VIA.

---

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 (Sept. 10, 2020), https://epic.org/apa/comments/EPIC-EU-Commission-AI-Sep2020.pdf.

[9] NITRD, *Research and Development Opportunities in Video and Image Analytics* ii (Mar. 2020).
[10] *Id*. at 2.

Dangerous use cases of VIA are many and widespread, including facial recognition algorithms and autonomous or AI-powered weapons systems.[11] For example, Project Maven, a Department of Defense R&D effort to develop wide area motion imagery technology for use in weapons systems, is still ongoing[12] despite mounting criticism and Google's high-profile withdrawal from the program in 2018 over human rights concerns.[13] The Department of Homeland Security (DHS) has also faced significant backlash[14] and criticism from EPIC and other organizations[15] for its introduction of facial recognition technology in airports. In a bipartisan letter to DHS, Sen. Ed Markey and Sen. Mike Lee raised privacy concerns and questioned the accuracy of DHS's system.[16]

NITRD NCO correctly acknowledged these risks by referencing Executive Order 13,960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, in the Request for Information.[17] In the updated version of the Action Plan, NITRD NCO should add a seventh strategic goal of safeguarding privacy and human rights in federal VIA R&D research.

One way to structure this seventh goal is to incorporate the Universal Guidelines for Artificial Intelligence ("UGAI") as baseline framework for the responsible governance of VIA R&D. The UGAI, based on the protection of human rights, were set out at the 2018 Public Voice

---

[11] *See* EPIC, *Ban Face Surveillance* (2022), https://epic.org/campaigns/ban-face-surveillance/; EPIC, *Face Surveillance and Biometrics* (2022), https://epic.org/issues/surveillance-oversight/face-surveillance/.

[12] Justin Doubleday, *Pentagon shifting Project Maven, marquee artificial intelligence initiative, to NGA*, Fed. News Network (Apr. 26, 2022), https://federalnewsnetwork.com/intelligence-community/2022/04/pentagon-shifting-project-maven-marquee-artificial-intelligence-initiative-to-nga/.

[13] Drew Harwell, *Google to Drop Pentagon AI Contract After Employee Objections to the 'Business of War,'* Wash. Post (June 1, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/google-to-drop-pentagon-ai-contract-after-employees-called-it-the-business-of-war/. *See generally* Melissa Heikkilä, *Why Business is Booming for Military AI Startups*, MIT Tech. Rev. (July 7, 2022), https://www.technologyreview.com/2022/07/07/1055526/why-business-is-booming-for-military-ai-startups/.

[14] Davey Alba, *The US Government Will Be Scanning Your Face at 20 Top Airports, Documents Show*, BuzzFeed News (Mar. 11, 2019), https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for.

[15] *E.g.*, *Assessing CBP's Use of Facial Recognition Technology: Hearing Before the H. Comm. on Homeland Sec. Subcommittee on Border Sec., Facilitation, & Ops.*, 117th Cong. 3–4 (2022) (statement of Jeramie Scott, EPIC Senior Counsel), https://homeland.house.gov/imo/media/doc/scott_testimony_bsfo_072722.pdf.

[16] *Id*.

[17] RFI, *supra* note 1.

meeting in Brussels, Belgium.[18] The UGAI have been endorsed by more than 250 experts and 60

organizations in 40 countries.[19] The twelve guidelines are:

1. Right to Transparency.
2. Right to Human Determination.
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.[20]

Among other key principles, the UGAI states: "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" (Right to Transparency); "Institutions must ensure that AI

systems do not reflect unfair bias or make impermissible discriminatory decisions" (Fairness

Obligation); "An AI system should be used 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" (Assessment and Accountability Obligation); "Institutions must ensure the accuracy,

reliability, and validity of decisions" (Accuracy, Reliability, and Validity Obligations); and

"Institutions must establish data provenance and assure quality and relevance for the data input into

algorithms" (Data Quality Obligation). Although not all VIA technologies rely on AI or make

determinations that bear directly on the rights of individuals, NITRD NCO should ensure that VIA

---

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

R&D and technologies which meet this description fulfill the human rights requirements of the UGAI.

Similarly, we urge NITRD NCO to give careful consideration to the National Institute of Standards and Technology's AI Risk Management Framework (AI RMF) in its updates to the Action Plan. The AI RMF is a guidance document designed to "preserve civil liberties and rights, and enhance safety while creating opportunities for innovation and realizing the full potential of [AI]."[21] Although the AI RMF is still under revision, it is a valuable resource that closely tracks the tenets of the UGAI, including trustworthiness, reliability, fairness, transparency, explainability, accountability, and privacy protection. It is essential that VIA R&D, as well as the systems and innovations that emerge from such R&D, be subject to the robust privacy and human rights safeguards reflected in the UGAI and AI RMF.

II. NITRD NCO should improve transparency as an element of the improved VIA R&D action plan.

Ensuring transparency in VIA R&D is key to the protection of privacy and human rights.[22] Under the UGAI, an AI system is transparent if 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."[23] Instilling transparency is also in line with the VIA R&D Action Plan's theme of securing uniformity across agencies.[24] A major goal of the 2020 Action Plan was to "improve communication and coordination across government agencies."[25] Under this umbrella, a short-term objective was to "create an index of R&D efforts, common vocabulary, shared portals,

---

[21] NIST, *AI Risk Management Framework: Second Draft* 2 (Aug. 18, 2022), https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.
[22] *Id*.
[23] *Id*.
[24] NITRD, *supra* note 9 at 5.
[25] *Id*.

products, and data across agencies to promote communication and collaboration."[26] The long-term objective was to create a common framework with government resources that included "best practices, access-controlled development frameworks, data and data modeling tools."[27] Although the 2020 Action Plan acknowledges the need for transparency between federal agencies engaged in VIA R&D, the revised version must ensure that this transparency extends to the public. The privacy and human rights risks of VIA technologies are significant—and growing. The public is owed a clear explanation of the VIA technologies being funded and developed by their own government and the information necessary to hold agencies accountable when VIA R&D poses an unacceptable threat to their rights.

III.   **Building consensus around binding limits on federal government VIA R&D should be a long-term objective of the Action Plan.**

In addition to coordinating between government agencies and private industry, NITRD NCO should involve civil society and the public in a process to establish binding privacy and human rights safeguards on VIA R&D and VIA technologies. In the short term, NITRD NCO should convene civil society and other stakeholders to develop privacy and human rights standards for the revised VIA R&D Action Plan. In the long term, NITRD NCO should work to establish binding safeguards on federal VIA R&D and the systems and innovations that emerge from such R&D. Again, NITRD NCO should look to AI governance best practices, like the Organization for Economic Co-operation ("OECD") and Development AI Principles,[28] to structure binding limits on VIA R&D.

---

[26] *Id*.
[27] *Id*.
[28] OECD, Recommendation of the Council on Artificial Intelligence (May 21, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

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]

The OECD framework is compatible with the Action Plan because it similarly anticipates a changing economy, market and "future analytic capabilities. . . ."[29] OECD recommends that governments "work closely with stakeholders to prepare for the transformation of the world of work and society."[30] EPIC supports the coordinated effort to regulate federal VIA R&D, but NITRD NCO must center privacy and human rights in the revision of the VIA R&D Action Plan in the short term and build consensus around binding limits on VIA R&D and VIA technologies in the long run.

IV. Conclusion

For the reasons above, NITRD NCO should include a seventh strategic goal in its revised Action Plan: centering privacy and human rights in VIA R&D. Additionally, EPIC urges NITRD NCO to ensure increased transparency of federal VIA R&D and work toward establishing binding privacy and human rights safeguards on VIA R&D. EPIC thanks NITRD NCO for its attention to

---

[29] NITRD, *supra* note 9 at 5.
[30] OECD, *supra* note 28.

these issues and for taking the time to consider EPIC's recommendations. If you have any questions,

please feel to contact John Davisson, EPIC Director of Litigation, at davisson@epic.org.

Respectfully,

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

/s/ Suzanne Bernstein
Suzanne Bernstein
EPIC Law Fellow