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 SCIENCE FOUNDATION

On Developing a Roadmap for the Directorate for Technology, Innovation, and Partnerships at the National Science Foundation

88 Fed. Reg. 26,345

July 27, 2023

The Electronic Privacy Information Center (EPIC) submits these comments in response to the National Science Foundation (NSF)'s April 28, 2023 request for information to aid its development of a roadmap for the Technology, Innovation, and Partnerships (TIP) Directorate.[1] The roadmap will guide investment decisions over a 3-year time frame with the ultimate goal of "advancing U.S. competitiveness in . . . key technology focus areas and addressing the identified societal, national, and geostrategic challenges."[2]

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age.[3] EPIC has a longstanding interest in federal efforts to develop privacy-protective technologies and regularly comments on federal planning efforts at the intersection of technology and privacy.[4]

To effectively and responsibly achieve the TIP Directorate's goals, EPIC makes the following recommendations: (1) the NSF should prioritize actionable artificial intelligence (AI) risk mitigation and oversight techniques; (2) the NSF should invest in strategies to increase and use of privacy enhancing

---

[1] NSF, Request for Information on Developing a Roadmap for the Directorate for Technology, Innovation, and Partnerships, 88 Fed. Reg. 26,345 (Apr. 28, 2023), https://www.federalregister.gov/documents/2023/04/28/2023-08995/request-for-information-rfi-on-developing-a-roadmap-for-the-directorate-for-technology-innovation.
[2] *Id.* at 26,345.
[3] *About Us*, EPIC (2023), https://epic.org/about/.
[4] *See, e.g.*, EPIC, Comments to NIST on the Request for Comment on De-Identifying Government Data Sets Paper (3rd Draft), (Jan. 13, 2023), https://csrc.nist.gov/publications/detail/sp/800-188/draft; EPIC, Comments To NSF on Request for Information on Federal Video and Image Analytics Research and Development Action Plan (Sept. 2, 2022), https://epic.org/documents/epic-comments-in- re-federal-video-and-image-analytics-research-development-action-plan/; EPIC, Comments to OSTP on Public and Private Sector Uses of Biometric Technologies (Jan. 15, 2022), https://epic.org/documents/epic-comments-to-ostp-on-public-and-private-sector-%20uses-of-biometric-%20technologies/; EPIC, Comments to NIST on Artificial Intelligence Risk Management Framework (Aug. 18, 2021), https://epic.org/documents/regarding-the-artificial- intelligence-risk- management-framework/; EPIC, Comments to OSTP & NIST on Request for Information on an Implementation Plan for a National Artificial Intelligence Research Resource (Oct. 1, 2021), https://epic.org/wp-content/uploads/2021/10/EPIC-Comment-NAIRR-Oct2021.pdf; EPIC, Comments to Comptroller of the Currency et al. on Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning (July 1, 2021), https://archive.epic.org/apa/comments/EPIC-Financial-Agencies-AI-July2021.pdf.

technologies (PETs); (3) the NSF should center privacy-preserving technologies as it develops and implements digital identity systems; and (4) the NSF should carefully consider and protect public access to crucial technologies developed by the U.S. government or with federal funds.

I. The NSF must prioritize investment and research into actionable AI risk mitigation and oversight techniques.

Today, many of the largest efforts to develop new and innovative AI technologies are within the private sector: massive technology companies like Microsoft and Google, as well as large data conglomerates like Thomson Reuters and LexisNexis, invest billions into the research and development of new AI and automated decision-making technologies.[5] While some of these AI developers have publicly supported efforts to regulate AI technologies[6] or made voluntary commitments to manage AI risk,[7] AI developers have long benefited from the federal government's laissez-faire approach to AI innovation, which frequently incentivizes innovation without regard to the risks or harms to the public.[8] As a result, everything from banks and schools to government services and hiring committees have turned to error- and bias-prone automated decision-making systems without understanding their proper uses, risks, and limitations.[9] The public deserves to feel safe and in control when operating or being subjected to AI and automated decision-making systems. The NSF is well-positioned to conduct actionable, translational research into the ways that new AI technologies can be used *ethically*, *responsibly*, and *fairly*.

Research into responsible AI development and use techniques are well-suited to NSF's use-inspired and translational research mandate. Despite years of research by academic scholars and advocacy organizations like EPIC on the risks and harms of AI and automated decision-making

[5] *See, e.g.*, Dina Bass, *Microsoft Invests $10 Billion in ChatGPT Maker OpenAI*, Bloomberg (Jan. 23, 2023), https://www.bloomberg.com/news/articles/2023-01-23/microsoft-makes-multibillion-dollar-investment-in-openai#xj4y7vzkg; Press Release, Thomson Reuters, Thomson Reuters Brings Forward Vision to Redefine the Future of Professionals with Content-Driven AI Technology (May 23, 2023), https://www.thomsonreuters.com/en/press-releases/2023/may/thomson-reuters-brings-forward-vision-to-redefine-the-future-of-professionals-with-content-driven-ai-technology.html (announcing investment of more than $100 million annually on AI).

[6] *See, e.g.*, David McCabe, *Microsoft Calls for A.I. Rules to Minimize the Technology's Risks*, N.Y. Times (May 25, 2023), https://www.nytimes.com/2023/05/25/technology/microsoft-ai-rules-regulation.html.

[7] Press Release, White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

[8] *See, e.g.*, EPIC, Comments to the White House Office of Science and Technology Policy on the Request for Information on National Priorities for Artificial Intelligence (July 7, 2023), https://epic.org/wp-content/uploads/2023/07/EPIC-OSTP-RFI-NationalPriorities.pdf; James Vincent, *White House Encourages Hands-off Approach to AI Regulation*, Verge (Jan. 7, 2020), https://www.theverge.com/2020/1/7/21054653/america-us-ai-regulation-principles-federal-agencies-ostp-principles. *Cf. generally* EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* (2023), https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf [hereinafter "Generating Harms Report"].

[9] *See* EPIC, Comments to the FTC on Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 70–75, 88–89 (Nov. 21, 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter "EPIC FTC Commercial Surveillance Comments"]; EPIC, *Screened & Scored in the District of Columbia* (Nov. 2, 2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf.

systems,[10] leading regulatory efforts to encourage responsible AI development and use still rely on voluntary efforts by companies that are incentivized to ignore the externalized costs of AI development.[11] Further, the viability and efficacy of AI risk management and oversight techniques are still widely debated. In its AI Risk Management Framework, the National Institute for Standards and Technology (NIST) highlights just some of the challenges inherent to implementing responsible AI development and use techniques, including challenges involving (1) methods for measuring the risks of third-party software, hardware, and data; (2) methods for tracking emergent risks; (3) disagreement over what the proper methods for measuring AI risk and trustworthiness should be; (4) changing risks at different stages of the AI development lifecycle; (5) differences between controlled development environments and the real word; (6) inscrutable or opaque AI decision-making; and (7) the propagation of human errors and bias in AI systems designed to augment or replace traditionally human decisions.[12] Research into metrics and techniques to overcome these challenges—as well as research into the efficacy and proper use contexts of specific oversight mechanisms like AI red-teaming, AI audits, training data sanitization procedures, and human-in-the-loop procedures[13]—will be crucial to ensure responsible AI development and minimizing the inequitable impacts of AI technologies.

Safety, privacy, innovation, and U.S. competitiveness need not be in conflict either.[14] Recent AI development has favored the mantra "move fast and break things" while eschewing privacy or safety mechanisms.[15] But prioritizing responsible AI development, testing, and use restrictions can spur new AI innovation and increase the competitiveness of U.S. technologies abroad. First, prioritizing research into and deployment of responsible AI practices forces AI developers to rethink limiting assumptions and historical practices instead of replicating existing processes.[16] Second, prioritizing investment and research into responsible AI development, use, and oversight can help ensure that new AI technologies developed within the U.S. can compete within more stringent regulatory environments like the European Union.[17]

By prioritizing translational research into AI risk management and oversight techniques and the implementation challenges they raise, the NSF will ensure not only that AI development conforms to domestic and international regulatory obligations, but also that the companies which purchase and use AI

---

[10] *AI & Human Rights*, EPIC (2023), https://epic.org/issues/ai/; *see also, e.g.*, Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793, 855 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Ctr. for Democracy & Tech. (July 7, 2021), https://perma.cc/L4ST-6C8D.

[11] Press Release, White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/; NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) (Jan. 28, 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [hereinafter "NIST AI RMF"].

[12] NIST AI RMF at 5–6.

[13] *See id.*; Generating Harms Report at 21, 24–29.

[14] *Cf.* Calli Schroeder et al., *We Can Work It Out: The False Conflict Between Data Protection and Innovation*, 20 Colo. Tech. L.J. 251, 259 (2022), https://ctlj.colorado.edu/wp-content/uploads/2023/02/3-We-Can-Work-it-Out_091922.pdf.

[15] *See* Sara Collins, *AI Doesn't Need to Move Fast and Break Things*, Pub. Knowledge (Apr. 7, 2023), https://publicknowledge.org/ai-doesnt-need-to-move-fast-and-break-things/.

[16] *See* Schroeder et al., *supra* note 14.

[17] *See, e.g.*, Shiona McCallum, *ChatGPT Banned in Italy over Privacy Concerns*, BBC (Apr. 1, 2023), https://www.bbc.com/news/technology-65139406.

technologies have the skills, knowledge base, and processes they need to deploy them *safely* and *effectively*. EPIC has forthcoming work on the role of federal funding and research in responsible AI development and would be happy to follow up with the NSF in the coming months with more specific input as well.

II. The NSF should devote research to Privacy-Enhancing Technologies.

The TIP Directorate investment roadmap should focus in part on developing and broadly implementing Privacy-Enhancing Technologies (PETs). As personal data continues to fuel our economy, it is critical to balance innovation with privacy protections for individuals. Some PETs achieve this by protecting individuals from reidentification attacks based on large data sets. Reidentification can pose various harms, including the disclosure of sensitive information about an individual or inferential disclosure concerning an entire class of individuals,[18] which can in turn result in embarrassment, identity theft, and other consequential injuries.[19] Other PETs are designed to minimize personal data sharing and ensure more robust data security. The NSF should devote research to (1) developing a national strategy for PETs at various levels of maturity, (2) educating and providing guidance to both government entities and private sector actors about PET use, and (3) developing implementation strategies for PETs to facilitate responsible adoption, translating research to practice.

PETs can be used in the data-driven economy or in research, government, and academic environments. Notable applications include financial transactions, healthcare, education, data management and transfers, research, digital advertising, and national security.[20] Across these contexts, data processing can vary from data-driven decision making, data sharing and analytics, to machine learning and artificial intelligence.[21] Based on the particular context and data use, the appropriate PETs can be incorporated into the data governance structures of companies and government organizations to strengthen data security and lower the risk of data misuse and abuse.

PETs range from highly technical to data accountability tools that limit data collection or enable data subjects to have control of their data.[22] Data obfuscation PETs like differential privacy, synthetic data, and zero-knowledge proofs add "noise" to data sets or remove identifying details to increase privacy protections.[23] Another category of PETs involve encryption. Encrypted data processing like homomorphic encryption and multi-party computation "allow data to remain encrypted while in use and thus avoiding the need to decrypt before processing."[24] It is also important to note a method gaining traction known as federated learning. This PET uses machine learning to collaborate on data sets without

[18] Simson Garfinkel et al., NIST, *De-Identifying Government Data Sets: Third Public Draft* 13 (2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-188.3pd.pdf.
[19] *Id*. at 1.
[20] *See* Cem Dilmegani, *Top 10 Privacy Enhancing Technologies & Use Cases in 2023*, AIMultiple (Dec. 21, 2022), https://research.aimultiple.com/privacy-enhancing-technologies/ (outlining use cases for privacy enhancing technologies).
[21] Information Commissioner's Office, *Privacy-Enhancing Technologies Guidance* 10-14 (2023), https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf (PETs in various types of data processing).
[22] Christian Reimsbach-Kounatze et al., *Emerging Privacy Enhancing Technologies: Current Regulatory & Policy Approaches*, 351 OECD Digit. Econ. Papers 5 (Mar. 2023), https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm.
[23] *Id*. at 4.
[24] *Id*.

sharing original data because "data is pre-processed at the data source."[25] In this way, federated learning enables data analysis without making the original data visible or accessible. Data minimization can also be understood as a PET. A data minimization framework limits data collection to what is reasonably necessary and proportionate to the primary purpose for which it was collected.[26] It can be broadly applied across organizations and industries to limit data security and privacy risks.

The NSF should invest in the continued development, awareness, and implementation of PETs across industries and government settings. The recent National Science and Technology Council (NSTC) report on Advancing Privacy-Preserving Data Sharing and Analytics (PPDSA) is an instructive resource to help achieve these goals.[27] Although the NSTC report focused mainly on PPDSA, its findings broadly support the potential of PETs to "catalyze American innovation and creativity by facilitating data sharing and analytics while protecting sensitive information."[28] The NSTC report also highlighted the timeliness for the expanded adoption of PETs as advances in emerging technology, including large language and generative AI models, continue to increase demand and value for data. "This landscape of technical capabilities, foundationally based on data, evolves daily and presents a unique moment for the convergence of techniques that fundamentally enhance privacy with those that are designed to derive insights from data."[29]

Through the TIP directorate roadmap, the NSF should invest in developing, educating, and providing guidance to implement PETs across government and industry. NSF Research can address some key challenges and roadblocks to reaching this goal. For example, the NSF could increase awareness of various PET methods by educating, producing materials to help others build expertise on definitions, taxonomies, implementation strategies and how PETs fit into regulatory compliance. Further research is needed to strengthen best practices for PETs, given the broad range of techniques and data processing environments. Ultimately, the NSF can play an important role in continuing to develop PETs and accelerating that research into practice.

III. In particular, the NSF should prioritize developing Privacy-Enhancing Technologies to enable digital identity.

Developing strong and privacy-preserving digital identity systems can improve U.S. economic competitiveness, reduce cybersecurity risks, and protect Americans. Digital identity is a rapidly developing field with a number of technologies that would benefit from near-term strategic investment, making these technologies a good fit for the NSF's goals. Broadly speaking, digital identity encompasses the range of interactions using technology to facilitate identity proofing (proving I am who I say I am), credentialing (proving I have authorization to do something), and digital transactions. There is also a substantial technical and policy overlap between digital identity and digital currencies like a government-issued central bank digital currency. Investing in privacy-preserving digital identity technology can promote the development of strong, privacy-preserving digital currencies as well.

---

[25] *Id*. at 5; *see also* National Science and Technology Council, *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics* 15 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf [hereinafter "NSTC Report"] (Table 1 Overview of PPDSA Capabilities).

[26] *See* EPIC FTC Commercial Surveillance Comments at 30–66 (introducing the concept of data minimization in the context of the FTC's commercial surveillance rulemaking).

[27] NSTC Report, *supra* note 25.

[28] *Id*. at 35.

[29] *Id*. at 12.

Digital identity standards and technology are evolving quickly; instead of identifying single standout technologies, we recommend that the NSF invest in a broad spectrum of technologies that have the potential to enable privacy-preserving digital identity systems. EPIC recommends that the NSF prioritize developing at least the following technologies that might form the backbone of near-future digital identity systems:

- Anonymous Credentials
- Digital Wallets
- Quantum-Computing Resistant Encryption
- W3C Verifiable Credential Compliant Digital Identity Products
- Zero-Knowledge Proofs

The Biden Administration recently identified advancing digital identity as a key strategic priory in the National Cybersecurity Strategy directing agencies to "[p]rioritiz[e] cybersecurity R&D for next-generation technologies such as postquantum encryption, digital identity solutions, and clean energy infrastructure."[30][31]

For further information on the importance of building maximally privacy-preserving digital identity infrastructure see the following resources:

- EPIC and ACLU Comments on Advancing Privacy in NIST's 2023 Digital Identity Guidelines (Apr. 14, 2023), https://epic.org/documents/epic-and-aclu-comments-on-nists-2023-digital-identity-draft-guidelines/;
- EPIC Comments to the White House OSTP on Digital Assets (Mar. 6, 2023), https://epic.org/documents/comments-of-epic-to-ostp-on-digital-assets-request-for-information/;
- Jay Stanley, *Identity Crisis: What Digital Drivers' Licenses Could Mean for Privacy, Equity, and Freedom*, ACLU (May 2021) https://www.aclu.org/report/identity-crisis-what-digital-drivers-licenses-could-mean-privacy-equity-and-freedom;
- EPIC Comments to NIST on Privacy Preserving Standards for Federal ID Cards (Feb. 2, 2021), https://epic.org/wp-content/uploads/apa/comments/EPIC-NIST-PIV-FIPS-Feb-2021-Comments.pdf.

EPIC also recommends the following guidelines for evaluating investment in digital ID tech and systems.

[30] Press Release, White House, FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy, (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/; White House, National Cybersecurity Strategy (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[31] *When will the phased digital ID rollout start? Which airports/states will be first in line for this new technology?*, TSA, https://www.tsa.gov/travel/frequently-asked-questions/when-will-phased-digital-id-rollout-start-which-airportsstates (last visited July 27, 2023).

a. Enable anonymous credentialling.

The best design for a universal digital identity system would allow for privacy-preserving authentication—i.e., would be compatible with anonymous credentials.[32] W3C Verifiable Credentials are compatible with anonymous credentialing. Anonymous credentials would, for example, allow a federal employee to convince a verifier that the employee has a security clearance without revealing any other information. The same system would allow someone presenting a mobile drivers' license at a liquor store to transmit only the information that the person is over the age of 21 and eligible to buy alcohol. In particular, anonymous credentials would prevent the identification from leaving behind a persistent identifier that would allow the individual to be linked to another authentication instance. This both safeguards the personal privacy of the person (so that even prying verifiers cannot trace this employee across many transactions) and protects secrets in government applications.

b. Avoid biometric-reliant digital identity.

Machine learning and generative AI are quickly creating a world where spoofing face and voice biometrics will be all too easy. The presence of these technologies requires escalating countermeasures, like the rapid spread of facial liveness testing, that increase barriers for individuals to access services.

Generative AI is already causing problems in the form of voice imposters and fake images that are difficult to identify. Recently, a deepfake image of Pope Francis in a full-length Balenciaga puffy coat made news internationally for its realistic feel.[33] The celebrity deepfakes trend underscores a growing threat vector for digital identity fraud: using generative AI to fake identity. In 2021, a study found that a common deepfake method called a generative adversarial network (GANs) could trick advanced facial recognition systems. In the study, deepfakes were able to pass facial recognition systems 85 to 95 percent of the time.[34] As generative AI improves, facial recognition will become increasingly susceptible to attack, which suggests that using facial recognition as the basis for remote identity verification is not a sustainable practice.

Voice biometrics are subject to similar, even simpler attacks. Earlier this year, journalist Joseph Cox was able to break into his own bank account using an AI-generated voiceprint.[35] Another journalist was able to fool an Australian government agency voiceprint system with generative AI.[36] And while voiceprints do not play a role in most current federal identity proofing, at least some agencies are exploring voiceprint identification. ICE's Alternatives to Detention program uses voiceprint recognition

---

[32] *See, e.g.*, Anna Lysyanskya, Signature Schemes and Applications to Cryptographic Protocol Design (Sept. 4, 2002), https://dspace.mit.edu/handle/1721.1/29271 (Ph.D. dissertation, MIT); Melissa Chase, *Efficient Non-Interactive Zero-Knowledge Proofs for Privacy Applications* (May 2008), http://static.cs.brown.edu/research/pubs/theses/phd/2008/chase.pdf, Fonteini Baldimtsi, Efficient Cryptography for Information Privacy (May 2014), https://cs.brown.edu/research/pubs/theses/phd/2014/baldimtsi.pdf (Ph.D. dissertation, Brown University); Endre Bangerter, Jan Camenisch, Anna Lysyanskaya, *A Cryptographic Framework for the Controlled Release of Certified Data*, 3957 LNCS 20–42 (2006), https://link.springer.com/chapter/10.1007%2F11861386_4.

[33] *See, e.g.*, Kalley Huang, *Why Pope Francis Is the Star of A.I.-Generated Photos*, N.Y. Times (Apr. 8, 2023), https://www.nytimes.com/2023/04/08/technology/ai-photos-pope-francis.html.

[34] *Id.*

[35] Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Vice (Feb. 23, 2023), https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice.

[36] Nick Evershed & Josh Taylor, *AI Can Fool Voice Recognition Used to Verify Identity by Centrelink and Australian Tax Office*, Guardian (Mar. 16, 2023), https://www.theguardian.com/technology/2023/mar/16/voice-system-used-to-verify-identity-by-centrelink-can-be-fooled-by-ai.

to verify the identity of migrants enrolled during regular check ins.[37] Outside of the federal government, voiceprint verification has spread rapidly in the last few years, especially in the banking industry.[38] Lawsuits over non-consensual use of voiceprint verification have also multiplied.[39]

Existing weaknesses in facial recognition have pushed identity verification providers to institute facial liveness testing in addition to facial recognition. But facial liveness is a largely unproven technology with no existing standards and has not been subjected to bias testing comparable to NIST's FRVT testing for facial recognition. At least some facial liveness products appear to have demonstrable biases, struggling to identify Black and Indigenous faces. The CBP One app rolled out for asylum seekers on the southern border includes a facial liveness test. Both migrants and immigrant-rights workers have documented a higher error rate for Black and Indigenous faces, especially when used in non-ideal lighting conditions.[40] Both ID.me and CBP One use iProov's facial liveness testing.[41]

The rise of facial liveness testing demonstrates that biometric verification will become increasingly complex and may result in an arms race between new biometric technologies and generative AI spoofs. Such a race is not good government policy. Constantly updating standards and technologies that mediate the relationship between the government and the public alienates users and creates additional barriers to accessing services. Similarly, introducing new and untested technologies will always create the risks of bias and error in new systems. Remote, repeat biometric collection is not a viable future-proof model for identity verification.

c. For near-term investments, require compliance with W3C Verifiable Credentials standards where appropriate.

The federal government does not have any universal standard for asserting a digital identity in place today. The two most commonly discussed digital identity standards are ISO/IEC mobile drivers licenses (mDLs)[42] and W3C Verifiable Credentials (VCs).[43] If the NSF is going to invest in compliance with a technical standard for remote identity verification, that standard should provide the individual with the greatest possible control over their information and the most robust privacy protections.

Currently, different components within the Department of Homeland Security (DHS) are working on implementing both mDLs and Verifiable Credentials in different applications. The TSA is

[37] DHS, Privacy Impact Assessment for the Alternatives to Detention (ATD) Program, DHS/ICE/PIA-062, 12–13 (Mar. 17, 2023), https://www.dhs.gov/sites/default/files/2023-03/privacy-pia-ice062-atd-march2023_1.pdf.
[38] Samantha Hawkins, *'Voiceprints' Roil Companies as Biometrics Litigation Skyrockets*, Bloomberg Law (May 18, 2022), https://news.bloomberglaw.com/privacy-and-data-security/voiceprints-roil-companies-as-biometrics-litigation-skyrockets; Jennifer A. Kingston, *Biometrics Invade Banking and Retail*, Axios (Feb. 18, 2020), https://www.axios.com/2020/02/18/biometrics-banking-retail-privacy.
[39] *Id.*
[40] John Washington, *Glitchy CBP One App Turning Volunteers Into Geek Squad Support for Asylum-seekers in Nogales*, AZ Luminaria (Mar. 20, 2023), https://azluminaria.org/2023/03/20/glitchy-cbp-one-app-turning-volunteers-into-geek-squad-support-for-asylum-seekers-in-nogales/.
[41] *See generally Government and Public Sector*, iProov, https://www.iproov.com/what-we-do/industries/government-and-public-sector (last visited July 27, 2023).
[42] ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application (Sept. 2021), https://www.iso.org/standard/69084.html.
[43] W3C Recommendation Verifiable Credentials Data Model v1.1 (Mar. 3, 2022), https://www.w3.org/TR/vc-data-model/.

currently piloting mDLs issued by several states at select checkpoints in the U.S.[44] Meanwhile U.S. Citizenship and Immigration Services, another DHS component, is developing a digital version of green cards enabled by W3C Verifiable Credentials.[45]

W3C Verifiable Credentials are a more privacy-protective standard than the ISO/IEC mDL standard. Importantly, verifiable credentials are designed to avoid a "phone home" where the entity verifying a person's identity directly contacts the issuer of the identifier. For example, a "phone home" when verifying a driver's license would call the DMV that issued the license to confirm its validity. Phoning home allows more expansive surveillance by both the issuer of the credential and the verifier. We recommend that the NSF rigorously evaluate, and if appropriate endorse the W3C standard. At a minimum, the NSF should not invest in any digital credentials that require or enable a phone-home.

IV. The NSF should carefully protect the public's access to crucial technologies developed using federal funds and personnel.

It is crucial that the public benefits fully when government scientists funded by taxpayer dollars co-develop crucial technologies with private sector partners. Intellectual property regimes such as patents are aimed at incentivizing private entities to produce useful technologies. But they come at a cost: patent-based monopolies lead to higher prices and lower availability for crucially important—and even lifesaving—technologies. The costs of this system may arguably be justified when, in its absence, useful inventions would not be produced. But when government agencies are ensuring technological development through direct research and funding, private industry should not be gifted sole monopoly power. Unfortunately, recent experience has shown that some companies will attempt to secure a windfall by wrongly denying that government scientists co-developed crucial technologies when applying for patents.[46] To ensure this does not happen with the next generation of crucial technologies brought about by the NSF, contractual terms with private industry partners must maintain a public option for development and distribution.

Public fights over ownership of the COVID-19 vaccine showcase the need for government to assert its role in technological development. During the height of the COVID-19 pandemic, when widespread access to vaccines was perhaps the most crucial factor for saving lives, biotech firm Moderna attempted to gain monopoly power over the vaccine, claiming in its patent application that government scientists did not co-invent the vaccine.[47] The scientific community referred to this as a "betrayal" given that NIH scientists and Moderna had worked together for four years to develop the technology and the government had provided Moderna nearly $10 billion in funding for the project.[48] Moderna, which had never successfully brought a vaccine to market before, claimed sole ownership of the patent, which would allow it to keep prices high by restricting the number of companies that could manufacture the vaccine.[49] Almost every company claims patent rights for its employees' inventions, and the federal government should do the same.

---

[44] *When will the phased digital ID rollout start? Which airports/states will be first in line for this new technology?*, TSA, https://www.tsa.gov/travel/frequently-asked-questions/when-will-phased-digital-id-rollout-start-which-airportsstates (last accessed July 27, 2023).
[45] DHS Sci. & Tech. Directorate, DHS Implementation Profile of W3C VCs and W3C DIDs (2022), https://lists.w3.org/Archives/Public/public-credentials/2022Sep/att-0253/DHS.W3C.VC-DID.Implemenation.Profile-20220929-SHARE.pdf.
[46] *See* Sheryl Gay Stolberg & Rebecca Robbins, *Moderna and U.S. at Odds Over Vaccine Patent Rights*, N.Y. Times (Nov. 9, 2021), https://www.nytimes.com/2021/11/09/us/moderna-vaccine-patent.html.
[47] *Id.*
[48] *Id.*
[49] *Id.*

To avoid a repeat of the Moderna fiasco, the federal government should set conditions in contracts with companies receiving its investments of funding and labor. To quote a recent piece from physician and sociologist Victor Roy:

> [T]o achieve public goals, the US government can use its position as a pivotal investor and buyer to set conditions in contracts. These conditions would relate to pricing and access, technology transfer, and reinvestment in innovation. The UK government, for example, negotiated pricing and access provisions with Astra-Zeneca during development of its covid-19 vaccine. The Bush administration created a program to transfer technology and scale-up for influenza vaccine manufacturing around the world in the mid-2000s. And for companies receiving government pandemic aid, US officials prohibited share buybacks and considered taking equity stakes to encourage reinvestment and a fairer return on public investment.[50]

The technologies described in this RFI will shape our world's future by addressing our responses to pandemics, climate change, and much more. It is crucial that access, distribution, and pricing decisions are made in the public interest. When the government is crucial for these technologies' coming into existence, it provides a useful path for ensuring that those values, not just profits, are considered.

V. Conclusion

EPIC applauds the NSF's efforts to establish the TIP directorate while considering various societal challenges that are related to advancing technology. Generally, the NSF should center privacy, risk mitigation, responsible oversight as it develops the TIP Directorate investment roadmap. EPIC encourages NSF to prioritize investment in: (1) AI risk mitigation and oversight frameworks; (2) privacy-enhancing technology use and education; (3) developing privacy-preserving digital identity techniques; and (4) protecting public access to US government funded and developed technologies. EPIC appreciates the opportunity to comment on the TIP Directorate roadmap, and we are eager to engage with the NSF further on any of the issues raised within our comment.

Respectfully submitted,

/s/ *John Davisson*
John Davisson
EPIC Director of Litigation

/s/ *Jake Wiener*
Jake Wiener
EPIC Counsel

/s/ *Thomas McBrien*
Thomas McBrien
EPIC Law Fellow

/s/ Suzanne Bernstein
Suzanne Bernstein
EPIC Law Fellow

/s/ Grant Fergusson
Grant Fergusson
EPIC Equal Justice Works Fellow

[50] Victor Roy, *Financing COVID-19 mRNA vaccines*, 380 BMJ 413 (2023), https://www.bmj.com/content/380/bmj.p413.short; *see also Taxpayers Paid Billions For It: So Why Would Moderna Consider Quadrupling the Price of the COVID Vaccine?: Hearing Before the S. Comm. on Health, Educ., Labor & Pensions*, 118th Cong. D251 (2023), https://www.help.senate.gov/imo/media/doc/Morten%20-%20Full%20written%20statement.pdf. (testimony of Christopher J. Morten, Associate Clinical Professor of Law, Columbia Law School).