Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on

Advancing Privacy Enhancing Technologies

Center for AI and Digital Policy (CAIDP)

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Center for AI and Digital Policy

Comments of the

THE CENTER FOR AI AND DIGITAL POLICY (CAIDP)
to the
OFFICE OF SCIENCE AND TECHNOLOGY POLICY (OSTP)
on the
THE PROMOTION OF PRIVACY-ENHANCING TECHNOLOGIES (PETs)

On behalf of the Center for AI and Digital Policy (CAIDP), we write in response to the Request for Information (RFI) on Advancing Privacy-Enhancing Technologies. [1] The CAIDP is an independent non-profit organization that advises national governments and international organizations on artificial intelligence (AI) and digital policy. The CAIDP currently serves as an advisor on AI policy to the OECD, the Global Partnership on AI, the Council of Europe, the European Union, and other international and national organizations. We work with more than 200 AI policy experts in over 50 countries.

The CAIDP has previously expressed strong support for AI policies that advance democratic values and promote broad social inclusion basedon fundamental rights, democratic institutions, and the rule of law.[2] In our report *Artificial Intelligence and Democratic Values*, we set out several recommendations for national governments.[3] In the U.S. country report, we noted favorably that the "U.S. and UK announced plans to promote Privacy Enhancing Technologies (PETs), including low-data AI, the deletion of unnecessary data, and techniques for robust anonymity."[4]

The Office of Science and Technology Policy (OSTP) has now issued a "Request for Information on Advancing Privacy-Enhancing Technologies.[5] We support the OSTP initiative.[6]

---

[1] "Request for Information on Advancing Privacy-Enhancing Technologies." *Federal Register: The Daily Journal of the United States Government*, The Office of Science and Technology Policy, June 6, 2022. https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies.
[2] CAIDP Statements, https://www.caidp.org/statements/
[3] CAIDP, *Artificial Intelligence and Democratic Values* (2022), https://www.caidp.org/reports/aidv-2021/
[4] Id. at 472.
[5] Id., supra 1.
[6] CAIDP wrote earlier to the OSTP in support of PETs. "New technologies such as AI pose new challenges for privacy, dignity, autonomy, and equality. Metrics for explainability, interpretability, and transparency should be established to protect fundamental rights, human

We agree that PETs can "promote continued innovation in emerging technologies in a manner that supports human rights and shared values of democratic nations."[7] We further support the goal "to accelerate the responsible development and adoption of PETs in a manner that maximizes the benefit to individuals and society, including increasing equity for underserved or marginalized groups and promoting trust in data processing and information technologies."[8] We believe this is one of the important challenges facing the United States in the realm of AI and digital policy.[9]

In these comments, we clarify the meaning of the critical term "Privacy Enhancing Techniques," place the current OSTP initiative in the context of other government efforts to promote PETs, identify examples of poorly conceived Privacy Enhancing Techniques, and warn that without adequate guidance many more unsafe systems will be deployed, placing users at risk and diminishing public confidence in this initiative. We make three specific recommendations:

1) Conduct independent evaluation of PETs prior to deployment
2) Promote expiration dates for commercial PETs
3) Incorporate PETs in the AI Bill of Rights

We need to underline at the outset that we use the term "Privacy Enhancing Technologies" precisely, as it was originally conceived, to describe **techniques that "minimize or eliminate the collection of personal data."**[10] This is also the definition adopted by the National Academies study on the HIPAA Privacy Rule which recommended that "the federal government should support the development and use of Genuine privacy-enhancing techniques

---

well-being, and to increase public trust. These metrics alongside Privacy Enhancing Technologies would help protect privacy." *Comments of CAIDP to OSTP on National Artificial Intelligence Research and Development Strategic Plan* at 4, Mar. 4, 2022 https://www.caidp.org/statements/ .

[7] Id., supra note 1.

[8] Id.

[9] In a statement to the US Congress, we set out a broad range of recommendations for the United States, including implementing the OECD AI Principles, establishing a process for meaningful public participation in the development of national AI policy, establishing an independent agency for AI oversight, establishing a right to algorithmic transparency, and supporting the Universal Guidelines for AI. *CAIDP Statement to House Armed Services Committee regarding US AI Policy* (Mar. 25, 2021), https://www.caidp.org/app/download/8305652763/CAIDP-HASC-03252021.pdf

[10] Marc Rotenberg, *Eurocrats Do Good Privacy: The contrast between a decorated cryptographer in Europe and one trying to avoid prosecution in the United States is more than curious,* Wired, May 1, 1996, (describing early government efforts to promote "Privacy Enhancing Technologies"), https://www.wired.com/1996/05/eurocrats/. See also Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision* in Technology and Privacy: the New Landscape 143–67 (eds., Philip E. Agre & Marc Rotenberg 1997);

that *minimize or eliminate the collection of personally identifiable data*."[11] As the OSTP itself has explained, examples of PETs include utilizing low-data artificial intelligence, deleting unnecessary data, and creating techniques for robust anonymity.[12] From this perspective, **the aim of PETs is not to enable further transfers of personal data but rather to limit the collection of personal data in the first instance**. There are many reasons to favor this approach

- Data breaches, criminal hacking, and espionage remain a primary concern for all organizations that choose to collect personal data.[13]
- Genuine PETs reduce privacy and security risks as data that is not collected cannot be misused by the data collector or be subject to data breach.[14]
- Genuine PETs protect vulnerable groups, particularly children. For example, President Biden recently called on Congress to "strengthen privacy protections, ban targeted advertising to children, and demand tech companies stop collecting personal data on our children."[15]
- Genuine PETs are aligned with well-established privacy norms, including the GDPR and many US privacy laws.[16]
- PETs typically seek to implement Fair Information Practices, and where possible, to minimize or eliminate the collection of personally identifiable information.[17]

---

[11] The Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research,* Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin, Editors 55 (2009) (Recommendation IIIa) (emphasis added)

[12] "U.S. and U.K. Governments Collaborate on Prize Challenges to Accelerate Development and Adoption of Privacy-Enhancing Technologies." *The White House*, The United States Government, 14 June 2022, https://www.whitehouse.gov/ostp/news-updates/2022/06/13/u-s-and-uk-governments-collaborate-on-prize-challenges-to-accelerate-development-and-adoption-of-privacy-enhancing-technologies/.

[13] IBM, *Cost of a Data Breach 2021* ("2021 had the highest average cost in 17 years: Data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the 17-year history of this report."), https://www.ibm.com/security/data-breach

[14] Testimony of Marc Rotenberg, *Privacy in the Commercial World,* U.S. House of Representatives, March 1, 2001 https://archive.epic.org/privacy/testimony_0301.html.

[15] The White House, *Remarks of President Joe Biden, State of the Union Address*, March 1, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/01/remarks-of-president-joe-biden-state-of-the-union-address-as-delivered/

[16] General Data Protection Regulation (GDPR), Art. 5(1)(c) (" Personal data shall be: . . . adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') (Principles relating to processing of personal data.)

[17] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy, (What Larry Doesn't Get),* 2001 Stan. Tech. L. Rev. 1 (2001). Marc Rotenberg, *Protecting Human Dignity in*

- Genuine PETs encourage the development of innovative techniques that are less dependent on the collection of personal data.[18]
- Genuine PETs minimize processing and are therefore aligned with emerging norms for AI policy that consider the environmental impact of big data models.[19]
- Genuine PETs are aligned with democratic values as they reduce the risk of mass surveillance.

We recognize that there are other techniques, including Privacy by Design and Privacy-Preserving Technologies (such as Differential Privacy) that incorporate techniques to enable the transfer of personal data. Where it is necessary to transfer personal data, the most robust methods should be adopted. That explains, for example, the central requirement that communications networks are built on end-to-end encryption.

We also respect the desire to enable data analysis for medical research and other fields of social benefit, but we caution that these same techniques for data aggregation can easily be used to enable mass surveillance and target vulnerable communities.[20] **The OSTP must be extremely cautious, in its efforts to promote data transfers, that it does not enable methods that could easily be turned against democratic values and marginalized communities.** As the OSTP itself has recently stated:

> [T]here are also risks that PETs could provide a false veneer of privacy, misleading people into believing that a data sharing arrangement is more private than it really is. Furthermore, in some cases, PETs could exacerbate existing problems with certain types of data analysis, such as discriminatory analysis resulting from biased data.[21]

---

the Digital Age, UNESCO (November 2000), https://unesdoc.unesco.org/ark:/48223/pf0000121984

[18] See, e.g., David Chaum, *Achieving Electronic Privacy,* Scientific American (August 1992) (Chaum developed techniques to provide authentication without identification, a cornerstone of the PETs paradigm as such techniques enable transactions without requiring the disclosure of personal data), https://www.scientificamerican.com/article/achieving-electronic-privacy/

[19] "Recommendation on the Ethics of Artificial Intelligence." *Unesdoc.unesco.org*, Nov. 23, 2021, https://unesdoc.unesco.org/ark:/48223/pf0000381137.

[20] Chris Buckley and Paul Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities,* NY Times, May 22, 2019, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

[21] The White House, Advancing a Vision for Privacy-Enhancing Technologies, June 28, 2022 https://www.whitehouse.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/

This concern should guide the OSTP's work in this field.

Subsequent Developments with PETS

The Madrid Privacy Declaration

Technical experts and civil society organizations have carried forward the effort to promote genuine Privacy Enhancing Technologies, based on the definition set out above. The Madrid Privacy Declaration of 2009, undertaken at the annual meeting of the Data Protection commissioners, reaffirmed international instruments for privacy protection, identified new challenges, and called for concrete actions.[22] The Madrid Declaration was endorsed by over 100 organizations and 200 experts. Among other recommendations, the Declaration "Reaffirm[ed] support for *genuine Privacy Enhancing Techniques that minimize or eliminate the collection of personally identifiable information* and for meaningful Privacy Impact Assessments that require compliance with privacy standards." The Declaration also "Recommend[ed] comprehensive research into the adequacy of techniques that deidentify data to determine whether in practice such methods safeguard privacy and anonymity."

These two recommendations – support for genuine PETS and research to evaluate such techniques – could be the cornerstone of the OSTP's work going forward.

The G20

Privacy Enhancing Technologies also arise in the context of global efforts to promote Data Free Flows with Trust (DFFT). The concept was developed by the recently deceased, former Japanese Prime Minister Shinzo Abe.[23] Prime Minister Abe underscored the importance of privacy protection, explaining that the DFFT regime should be built on "non-personal data."[24]The G20 nations, of which the US is a member, have endorsed this concept of PETs. At the 2020 G20 meeting the Digital Ministers stated:

> The cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development. At the same time, we recognize that the free flow of data raises certain challenges, such

[22] "Madrid Declaration." *The Public Voice*, Nov. 3, 2009, https://thepublicvoice.org/madrid-declaration.
[23] *Prime Minister Abe's AI Policy and Data Governance Legacy*, CAIDP Update 1.7 (Sept. 1, 2020), https://dukakis.org/center-for-ai-and-digital-policy/caidp-update-prime-minister-abes-ai-and-data-governance-legacy/
[24] Id.

> as the protection of privacy and personal data. G20 members recognize the need to address these challenges, in accordance with relevant applicable legal frameworks, which can further facilitate data free flow and strengthen consumer and business trust, without prejudice to legitimate public policy objectives, including by: . . . exploring and better understanding technologies such as privacy enhancing technologies (PETs).[25]

The G7

The G7 is another global forum that has promoted Privacy Enhancing Technologies.[26] The Data Protection and Privacy officials of the G7 nations also issued a statement on Data Free Flows with Trust which said, "human dignity, must be central to AI design; AI must be transparent, comprehensible, and explainable; and the data protection principles of purpose limitation and data minimization must apply to AI." They said that "'red lines' are needed for AI systems that are not compatible with our values and fundamental rights."[27]

1) The Need for Independent Evaluation of PET

PETs offer great promise. However, it is necessary to ensure that there is independent evaluation of these techniques prior to deployment. Companies and government agencies should not be allowed to represent that they have established Privacy Enhancing Techniques without independent evaluation. Several consumer privacy cases, as well as government surveillance programs, have demonstrated the shortcomings of that approach.

For example, in 2008, the FTC sued Ask.com for misrepresenting the privacy technique for the search engine AskEraser, after a group of consumer privacy organization identified flaws in the privacy technology.[28] As the organizations explained:

> The company purports to provide an Internet search engine that provides privacy protection by limiting the collection and use of Internet search histories. In fact,

[25] *Ministerial Declaration*, G20 Digital Economy Ministers Meeting, July 22, 2020, http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html.]
[26] *G7 Digital and Technology Track – Annex 2: G7 Roadmap for Cooperation on Data Free Flow with Trust,* Apr 28, 2021, http://www.g8.utoronto.ca/ict/2021-annex_2-roadmap.html
[27] G7 United Kingdom 2021, *Data Free Flows with Trust*, Sept. 8, 2021, https://www.caidp.org/app/download/8342900463/g7-attachment-202109.pdf
[28] EPIC, Center for Digital Democracy, Consumer Action, Fairfax County Privacy Council, Patient Privacy Rights, U.S. Bill of Rights Foundation, *In the Matter of Ask.Com, Complaint and Request for Injunction, Request for Investigation and for Other Relief*, Jan. 19, 2008, https://epic.org/wp-content/uploads/privacy/ask/epic_askeraser_011908.pdf

> the product does not work as advertised: Internet search histories will be retained without notice to Internet users. Moreover, AskEraser requires Internet users to disable genuine privacy features, and it exposes Internet users to additional tracking, monitoring, and profiling by means of a Persistent Identifier.

Ask.com claimed that AskEraser, would delete search histories "within hours." The company advertised that the new search tool "will offer its searchers unmatched control over their privacy." However, Ask.com placed a persistent unique identifier, also known as a "cookie," on the user's device that would be stored for two years. With the persistent identifier, the company gathered sensitive personal data such as IP addresses, the address of the last URL visited before arriving at Ask.com. And the company actually prevented users from deleting the persistent identifier if they were to use the service. As a consequence, Ask.com "privacy technique" allowed the company to track and monitor the user for as long as the user continued to use the service. The FTC determined that this was an unfair and deceptive trade practice.[29]

A similar problem arose with Snapchat, a social media app which claimed that users could make photos 'vanish."[30] In fact, an investigation revealed that the photos were retained. Snapchat also transmitted users' location data and collected their address books without consent. According to the Electronic Privacy Information Center (EPIC), Snapchat made multiple misrepresentations to consumers about its product that stood in stark contrast to how the app actually worked. The Federal Trade Commission agreed with EPIC, pursued an investigation, and obtained a settlement.[31]

---

[29] *In the Matter of Snapchat, Inc.*, No. C-4501, before the Federal Trade Commission, Dec. 23, 2014, https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf

[30] *Privacy watchdog EPIC files complaint against Snapchat with FTC,* Los Angeles Times, May 17, 2013 ("Snapchat is the app that promises to delete photos but it doesn't," said Marc Rotenberg, EPIC's executive director. "We have no problem with apps that make photos vanish. But they should work as promised, and if they don't the Federal Trade Commission should investigate."), https://www.latimes.com/business/la-xpm-2013-may-17-la-fi-tn-privacy-watchdog-epic-files-complaint-against-snapchat-with-ftc-20130517-story.html; EPIC, *In the Matter of Snapchat: Complaint, Request for Investigation, Injunction, and Other Relief,* May 16, 2013, ("Despite promising to its users that photos and videos sent via Snapchat will 'disappear forever,' Snapchat photos and videos remain available to others even after users are informed that the photos and videos have been deleted.") https://epic.org/wp-content/uploads/privacy/ftc/EPIC-Snapchat-Complaint.pdf

[31] Federal Trade Commission, *Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False: Snapchat Also Transmitted Users' Location and Collected Their Address Books Without Notice Or Consent,* May 8, 2014, https://www.ftc.gov/news-events/news/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were-false. See also Andrea Peterson*, Snapchat agrees to settle FTC charges that it deceived users*, The

The examples of AskEraser and Snapchat demonstrate that there must be independent evaluation of Privacy Enhancing Techniques. Any strategy for PETs that fails to incorporate such safeguards will almost certainly encourage faulty technology, place users at risk, and diminish public support for the initiative.

A related problem concerns the definition of PETs. For example, the recent US-UK initiative relies on a loose definition of "PETs" to justify what will likely be massive collections of personal data by law enforcement agencies. UK Minister Julia Lopez, said that she was "delighted that the U.K. and U.S. are working with regulators on both sides of the Atlantic to help realize the potential of novel privacy-enhancing technologies (PETs) to tackle financial crime." She went on to describe how the U.K.'s National Data Strategy outlines "the promise of trustworthy data access." According to the UK official, "PETs have the potential to facilitate new forms of data collaboration to tackle the harms of money laundering, while protecting citizens' privacy."[32] But the obvious question that needs to be considered is what mechanisms of oversight will be established to ensure that citizens privacy will be protected when law enforcement agencies are in control of the privacy technologies. In most simple terms, "who will watch the watchers?" If that question cannot be answered at the outset, such programs should not go forward.

There are many examples were such representations of privacy preserving techniques by government agencies turned out, on closer inspection, to be false. For example, the US federal agencies responsible for the development of wiretapping techniques in the 1990s, known as "Carnivore," claimed that the only data that would be accessed was the data lawfully accessible under a judicial warrant. But independent investigation revealed that the data could be obtained by government officials outside the scope of the warrant.[33] Similarly, the developers of the Total Information Awareness program claimed that they had established privacy safeguards but that was only with regard to data access by low-level government employees and did nothing to limit

---

Washington Post, May 8, 2014 ("Julia Horwitz, Consumer Protection Counsel at the Electronic Privacy Information Center which originally complained to the FTC about Snapchat, told the Post it was happy with the resolution. 'We're extremely pleased that the FTC is taking its data privacy protection seriously and is recognizing behaviors by companies like Snapchat that breach promises to consumers,' she said. 'This was a real success. But this consent order's true effectiveness depends upon the agency's consistent enforcement over the next 20 years,' she cautioned.")

[32] "U.S. and U.K. Governments Collaborate on Prize Challenges to Accelerate Development and Adoption of Privacy-Enhancing Technologies." *The White House*, The United States Government, 14 June 2022, https://www.whitehouse.gov/ostp/news-updates/2022/06/13/u-s-and-uk-governments-collaborate-on-prize-challenges-to-accelerate-development-and-adoption-of-privacy-enhancing-technologies/.

[33] IIT Research Institute, *Independent Review of the Carnivore System*, Dec. 8, 2000, https://www.justice.gov/archive/jmd/carniv_final.pdf

the ability of department heads to repurpose the use of the data collected. More recently implementation of the Cyber Information Sharing Act has been subject to scrutiny precisely because it enables the transfer of personal data to government agencies outside the judicial process, relying on novel techniques for privacy protection.

Another project of concern is currently underway at the Global Partnership on AI (GPAI). The GPAI is investigating the use of AI-powered cameras for surveillance and monitoring of outdoor and working environments.[34] The intention is that the cameras will be programmed to intervene if specified events are detected, such as a fire or medical emergency. But of course, this is also a system of mass surveillance that will capture the images and conversations of identifiable individuals in real time. The technical challenge will be to eliminate the massive amount of personal data that will be routinely gathered with the goal of identifying the events of interest without compromising privacy. But the organizational challenges, rarely considered at the outset, will be to prevent the reuse of the data gathered for other unrelated purposes.

A simpler and more effective solution may be simply to avoid systems that involve the massive collection of unnecessary personal data and deploy instead techniques that are specifically designed to identify the risk of fire or to alert personnel in the case of medical emergencies. These techniques are likely to be more reliable, more effective, less complex, and less expensive. A device designed solely to detect fire, as compared with a general-purpose system that gathers massive amounts of personal data, is an excellent example of a PET as it would accomplish its task without collecting unnecessary personal data.

2) The Need for Expiration Dates for PETs

In addition to independent evaluation for PETs, we also strongly recommend a certification program that would indicate a time period during which the security of the PET would be assured. This is necessary because rapid advances in cryptography and data analytics have made clear that popular techniques will over time no longer be secure. For example, MD5 a popular cryptographic hashing function, developed by Ron Rivest in 1991, was later found to have extensive vulnerabilities.[35]

A National Academies of Sciences study that seeks to promote Privacy Enhancing and Privacy-Preserving Techniques recommended the use of expiration dates to provide legal certainty for those who offer and deploy Privacy Enhancing Techniques.[36] We support this

[34] "AI at Work Observation Platform." *GPAI*, Nov. 2021, https://gpai.ai/projects/future-of-work/ai-at-work-observation-platform/.
[35] Wikipedia, MD5, https://en.wikipedia.org/wiki/MD5
[36] Robert M Groves, Michael E Chernew, Piet Daas, Cynthia Dwork, Ophir Frieder, Hosagrahar V Jagadish, Frauke Kreuter, Sharon Lohr, James P Lynch, Colm O'Muircheartaigh, Trivellore

proposal and recommend that it be incorporated in the OSTP initiative to promote Privacy Enhancing Technologies.

3) Advancing PETs in the Context of the AI Bill of Rights

Finally, we recommend that the OSTP advance Privacy Enhancing Technologies in the context of the AI Bill of Rights much as civil society organizations and technology experts promoted Privacy Enhancing Technologies and related research in the context of the Madrid Privacy Declaration. *The AI Bill of Rights should incorporate an affirmative obligation to adopt Privacy Enhancing Techniques that have been subject to independent review and a privacy impact assessment.*

Conclusion

We support the OSTP initiative to promote Privacy Enhancing Technologies. Such techniques are particularly important as more services are digitized and more data is gathered. But we caution that genuine PETs will minimize or eliminate the collection of personal data. It is a fundamental conceptual mistake to assume that PETs are intended to facilitate the transfer of personal data.

Many of the great challenges facing our nation, including measuring the consequences of climate change, require virtually no collection of personally identifiable information.[37] But the collection of personal data poses specific challenges that cannot be ignored as the OSTP itself has acknowledged. The precise definition of Privacy Enhancing Techniques will help ensure that the social benefits are maximized, the risks to democratic values and marginalized groups ae minimized, and true innovation occurs.

Thank you for your consideration of our views. We welcome to opportunity to discuss further.

Raghunathan, Roberto Rigobon, and Marc Rotenberg. 2017. *Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy,* National Academies of Sciences, Engineering, and Medicine paper, https://privacytools.seas.harvard.edu/publications/innovations-federal-statistics-combining-data-sources-while-protecting

[37] Marc Rotenberg*, Let's Use Government Data to Make Better Policy: It's a no-brainer, as long as privacy concerns are taken seriously,* Scientific American (Oct. 4, 2017), https://blogs.scientificamerican.com/observations/let-rsquo-s-use-government-data-to-make-better-policy/

Sincerely,

Marc Rotenberg CAIDP President	Merve Hickok CAIDP Chair	Karine Caunes CAIDP Global Program Director

/S/

Dr. Lorraine Kisselburgh CAIDP Board Members	Maison Bergeron CAIDP Research Assistant	Sandra Lattner CAIDP Research Assistant

Center for AI and Digital Policy
1100 13th St., NW, Suite 800
Washington, DC 20005
caidp.org