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

Future of Privacy Forum

FUTURE OF PRIVACY FORUM
1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

July 8, 2022

Office of Science and Technology Policy (OSTP)
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504
VIA EMAIL: PETS-RFI@nitrd.gov
Attention: Ms. Stacey Murphy

RE: RFI Response: Privacy-Enhancing Technologies, Doc. No. 2022-12432

The Future of Privacy Forum (FPF) welcomes this opportunity to share our thoughts regarding specific actions that would advance the adoption of privacy-enhancing technologies (PETs). FPF is a 501(c)(3) non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Our primary office is in Washington, DC, and we work closely with our colleagues in Brussels, Singapore, Tel Aviv, and around the world. FPF seeks to support balanced, informed public policy.[1]

In response to the Office's invitation for comments, and with regard for the particular categories of information requested,[2] FPF recommends that the OSTP include the following three recommendations in the national strategy on privacy-preserving data sharing and analytics:

1. Support the growing discipline of privacy engineering aimed at bridging the gap between technologies and policies through direct funding of academic research, building expertise within government, encouraging business-academia dialogues, and directing agencies to require federal contractors to incorporate PETs as appropriate to promote common standards in the discipline.;

2. Recommend the establishment of a trusted inter-agency and multi-stakeholder body, including the FTC, NIST, HHS, NSF, and experts from the private sector, civil society, and academia, to provide guidance and standards-setting for de-identification and the role of PETs, with particular regard to their utility for compliance with state and federal legislation; and

[1] The views herein do not necessarily reflect the views of our supporters or Advisory Board.
[2] Office of Science and Technology Policy, *Request for Information on Advancing Privacy-Enhancing Technologies*, Federal Register, (June 9, 2022), Accessed June 25, 2022, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies.

3. Encourage the establishment of Administrative Data Research Networks (ADRNs) that offer de-identification tools to facilitate researcher access to data in a secure manner.

Each of the next three sections correspond to one of these recommendations, exploring a barrier to PET's adoption and providing further information about the recommendations that address these issues. Below each section header, the topics implicated by a recommendation are identified by the corresponding number in the RFI. FPF hopes that this filing provides the Office with an enhanced understanding of this space and informs solutions.

1. Supporting Privacy Engineering as a Discipline Through Agency Funding of Research, Building Expertise Within Government, Greater Industry-Academia Dialogue, and PETs Requirements in Federal Contracting.

Relevance: Topics 6 and 9.

A national strategy for advancing privacy-enhancing technologies (PETs) should first aim to support the privacy engineering discipline to build the applied technical expertise needed to support the growth of privacy-enhancing technology in the United States. Organizations are increasingly engaging in the extensive collection and processing of data to enable data-driven products and services. The privacy issues raised by data processing have coincided with governments passing new laws regulating this activity, which has created a new global industry for "privacy tech."[3]

In support of the emerging privacy tech sector, there has been a sharp increase in demand for privacy engineering, a subfield within computer science committed to the development of technologies that facilitate compliant data flows under privacy and data protection law.[4]

[3] Privacy Tech Alliance, Future of Privacy Forum, Tim Sparapani, and Justin Sherman, *Privacy Tech's Third Generation - A Review of the Emerging Privacy Tech Sector*, Future of Privacy Forum, 37, (2021), Accessed June 27, 2022, https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf (noting that all seventeen respondents to the survey question "Has your company ever purchased privacy-enhancing technologies, whether software or hardware, from a third-party provider?" responded yes).

[4] *Id*. at 32 (describing how the PETs market has recently expanded to create "products and services that assist businesses in making the personal data they encounter both maximally available and maximally valuable for various components throughout the business . . . .").

However, despite the high demand for privacy engineers in the private sector, the academic field of privacy engineering is not currently aligned with market needs.[5] While there are some long-standing and some newly emerging privacy engineering conferences, very few academic institutions currently offer certifications or graduate programs in privacy engineering.[6] The lack of opportunities for practitioners to obtain necessary skills creates a shortage of talent who can develop these technologies.[7] Even when such talent is being developed or already exists, researchers may be pursuing certifications or skills that are not aligned with companies' PETs needs.[8] Furthermore, there are typically few opportunities for meaningful interaction between industry practitioners and academic technologists studying privacy engineering.[9]

- **Recommendation:** A national strategy for PETs should support the growing discipline of privacy engineering aimed at bridging the gap between technologies and policies through direct funding of academic research, building expertise within government, encouraging business-academia dialogues, and directing agencies to require federal contractors to incorporate PETs as appropriate to promote common standards in the discipline.

A national strategy should seek to bridge the gulf between academic talent and market demand through funding privacy engineering research, increasing opportunities for business-academic dialogue, building capacity within the US Government, and fostering growth of the field through requirements of federal contractors. Federal agencies can directly support academic opportunities through funding of privacy engineering research,[10] which would increase the demand for privacy technologists and make academic career paths in privacy engineering more attractive. Federal agencies can build

---

[5] Privacy Tech Alliance et al., *supra* note 3, at 22, ("Several buyers with whom we spoke identified the nascency of privacy engineering as one constraint on in-house privacy tech development. Simply put, there may not be enough privacy engineering talent to go around in general.").

[6] Carnegie Mellon University, *Privacy Engineering Program*, Accessed July 6, 2022, https://privacy.cs.cmu.edu, (Carnegie Mellon University is one of the few examples of an academic institution that provides training and certifications for privacy engineers).

[7] *See* Privacy Tech Alliance et al., *supra* note 3, at 22.

[8] *See* Jules Polonetsky and Jeremy Greenberg, *NSF Convergence Accelerator Paper: The Future of Privacy Technology*, Future of Privacy Forum, 12, (2020), Accessed June 27, 2022, https://fpf.org/wp-content/uploads/2020/03/NSF_FPF-REPORT_C-Accel 1939288_Public.pdf, ("In a separate meeting with 15 companies that provide privacy tech tools for compliance, few of these companies were familiar with academic research or scientific advances in their particular focus area. As one of the academic observers at our New York City meeting commented, we need to address the academic to practitioner (and reverse) relationship 'if we are serious about convergence.'").

[9] *Id.*

[10] Legislation that promotes research into PETs could play a useful role. For example,the "Promoting Digital Privacy Technologies Act" (H.R.847), introduced in February 2022 by Representative Haley Stevens (D-MI) passed the US House of Representatives in May 2022.

dedicated internal capacity for privacy engineering; both CISA and the CIO Council have pursued valuable capacity building efforts regarding cybersecurity expertise that can serve as partial models.[11] In addition, agencies can create increased opportunities through workshops, forums, competitions, and conferences, for businesses and academic researchers to exchange ideas and collaborate on innovation in privacy enhancing technology. This could help achieve greater alignment between skills development and market needs.

Finally, a national strategy driven by the OSTP can support widespread PETs adoption by encouraging agencies to require PETs as a precondition for federal contractors placing bids on certain projects. Agencies could use this method to establish standards for PETs that businesses must comply with. Privacy engineers may then create or adopt PETs based on the federal benchmark, leading to a national standard for the market.

2. Promoting Definitional Clarity and Creating Consensus Around What De-Identification Methods Satisfy Legal Requirements Using a Trusted Inter-Agency and Multi-Stakeholder Body.

Relevance: Topics 2, 6, and 7.

A national strategy to advance privacy-enhancing technologies (PETs) should also seek to promote greater definitional clarity and consensus around what de-identification methods satisfy legal requirements. Many—but not all[12]—PETs[13] are designed to enable de-identification, or the reduction of the identifiability of datasets. De-identification methods are a central aspect of all modern data processing, including healthcare

[11] *See e.g.*, Cybersecurity and Infrastructure Security Agency, *Capacity Enhancement Guides for Federal Agencies*, CISA, Accessed July 7, 2022, https://www.cisa.gov/capacity-enhancement-guides-federal-agencies; U.S. CIO Council, *Chief Information Officers Council Handbook*, 124, Accessed July 7, 2022, https://www.cio.gov/assets/files/Handbook-CIO.pdf.

[12] Cem Dilmegani, *Top 10 Privacy Enhancing Technologies (PETs) & Uses in 2022*, AI Multiple, (June 14, 2022), Accessed on July 7, 2022, https://research.aimultiple.com/privacy-enhancing-technologies/, (Although some PETs, such as federated learning models and homomorphic encryption, resolve a key aspect of data privacy by allowing for learning *without* the collection or sharing of data, many other privacy enhancing technologies are designed for the de-identification of existing datasets).

[13] Office of Science and Technology Policy, *Advancing a Vision for Privacy-Enhancing Technologies*, OSTP Blog, (June 28, 2022), Accessed July 6, 2022, https://www.whitehouse.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/, (defining PETs as "technologies that will allow researchers, physicians, and others permitted access to gain insights from sensitive data without ever having access to the data itself.").

research,[14] assessments of corporate diversity and inclusion efforts,[15] and product and service improvements.[16]

In general, de-identification methods, from blurring or suppressing data to more robust techniques such as differential privacy, share a similar goal of preserving utility of data while promoting privacy. Sometimes, this balance is poorly struck. Strong de-identification may protect privacy but prevent organizations from uncovering important insights from data. For example, differential privacy may underestimate bias when the size of a dataset changes.[17] In other circumstances, de-identification methods may not provide a sufficient level of privacy while retaining the underlying utility of data. Some data sets are particularly difficult to de-identify in ways that appropriately reduce the risk of re-identifying individuals while retaining information needed for socially beneficial research. For example, it remains difficult to de-identify individualized location data[18] while

[14] Simon L. Garfinkel, *De-Identification of Personal Information*, NIST, 1, (2015), Accessed June 28, 2022, https://csrc.nist.gov/publications/detail/nistir/8053/final, ("[S]ignificant medical research resulting in societal benefit is made possible by the sharing of de-identified patient information under the framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule . . . .").
[15] SafePorter, Accessed June 28, 2022, https://www.safeportersecure.com.
[16] Apple, *Differential Privacy*, 1–2, Accessed June 27, 2022, https://www.apple.com/privacy/docs/Differential_ Privacy_Overview.pdf, (noting that Apple uses a differential privacy technique to learn about user's behaviors for purposes of improving device features, such as auto-correction and predictive text-entry, without connecting those behaviors to people).
[17] Heng Xu and Nan Zhang, *Implications of Data Anonymization on the Statistical Evidence of Disparity*, Management Science (accepted), ec6, (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662612 (stating that "when disparity was operationalized through separation . . . noise insertion [differential privacy is a noise insertion technique] likely produces false negatives only, with false positives being highly unlikely.").
[18] Simon L. Garfinkel, *supra* note 14, at 37, ("Without some kind of generalization or perturbation, there is so much diversity in geographic data that it may be extremely difficult to de-identify locations."); Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Nature, 4, (2013), https://www.nature.com/articles/srep01376, ("[T]he uniqueness of human mobility traces is high, thereby emphasizing the importance of the idiosyncrasy of human movements for individual privacy. Indeed, this uniqueness means that little outside information is needed to re-identify the trace of a targeted individual even in a sparse, large-scale, and coarse mobility dataset.").

preserving its utility for a range of purposes, including public health surveillance and contact tracing.[19]

Overall, one of the greatest barriers to widespread adoption of de-identification technologies has been the lack of regulatory certainty about legal definitions and standards for de-identification. Because privacy and data protection laws typically do not apply to personal data that has been de-identified,[20] the legal standards related to "de-identified data" are a subject of considerable international legal and policy debate. For example, the Health Insurance Portability and Accountability Act (HIPAA) provides a legal Safe Harbor for de-identification of medical records that is typically thought to differ from the standard of "anonymization" under the European Union's General Data Protection Regulation (GDPR), a standard which is again likely different from the emerging legal standards in state privacy laws such as the California Consumer Privacy Act (CCPA).[21] Given this regulatory uncertainty, many US businesses express reservations about investing in PETs due to confusion about whether they will effectively shield them from regulator scrutiny.

In addition to generating legal uncertainty, the lack of consensus makes it harder for market participants to have conversations about these tools, frustrating adoption.[22] Furthermore, many organizations do not understand which use cases would benefit from

---

[19] Stacey Gray, *A Closer Look at Location Data: Privacy and Pandemics*, Future of Privacy Forum, (March 25, 2020), Accessed June 27, 2022, https://fpf.org/blog/a-closer -look-at-location-data- privacy-and-pandemics/, ("Because location data is sensitive and challenging to truly "de-identify" (i.e. to significantly reduce or eliminate all privacy risks), there is a serious concern that once collected by a public health agency for pandemic tracking, it could be retained or used for other purposes. . . . [Location data] should be clearly siloed for that purpose and not re-used or retained for other civil or law enforcement uses.").

[20] Jules Polonetsky and Jeremy Greenberg, *supra* note 8, at 2; Simon L. Garfinkel, *supra* note 12, at 4, noting that some "U.S. laws and regulations specifically recognize the importance and utility of de-identification." Examples include the Family and Educational Records Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule).

[21] *See* Privacy Tech Alliance et al., *supra* note 3, at 27, ("[P]seudonymization and de-identification . . . have different meanings in the US and the EU, including to what extent they are distinct. Even when regulatory or statutory terms start out with a common definition, differing interpretations of those terms by regulators or judges can cause divergence over time of the meaning of a common term in different states or countries.").

[22] Privacy Tech Alliance et al., *supra* note 3, at 12 (noting that "a lack of common, consensus privacy tech definitions" is limiting the adoption of privacy-enhancing technologies).

these technologies.[23] These questions are particularly salient for small or resource-constrained businesses, who may find it challenging to make the business case for adoption of de-identification PETs. In essence, siloed conceptions of de-identification create uncertainty surrounding how de-identification standards fit within existing legal requirements and when they should be used.

- **Recommendation:** A national strategy should recommend the establishment of a trusted inter-agency and multi-stakeholder body, including the FTC, NIST, HHS, NSF, and experts from the private sector, civil society, and academia, to provide guidance and standards-setting for de-identification and the role of PETs, with particular regard to their utility for compliance with state and federal legislation.

As part of a national strategy, the OSTP should support efforts that promote definitional clarity and create consensus around what de-identification methods satisfy legal requirements. To achieve these goals, the Office could direct an agency or group of agencies to establish a trusted body.[24] This body could take the form of a multistakeholder commission, including the FTC, NIST, HHS, NSF, and experts from the private sector, civil society, and academia. It would be responsible for providing guidance, recommendations, and standards for de-identification tools and other PETs.[25] As part of this work, the body should clarify how uses of PETs map onto legal requirements and analyze how these technologies are best utilized.[26] For example, this exercise could shed light on what constitutes de-identification under certain laws and which applications an organization should utilize a particular tool for.

---

[23] Jules Polonetsky and Jeremy Greenberg, *supra* note 8, at 3, ("Our initial survey included conversations at three meetings with privacy leads from a total of 40 companies. In each meeting, companies indicated significant interest in de-identification, but in most cases had limited awareness of the academic state-of-the-art. To the extent companies were versed in the basics of differential privacy or homomorphic encryption, ***they were unclear which use cases would benefit from these technologies . . .*** .") (emphasis added).

[24] Privacy Tech Alliance et al., *supra* note 3, at 6.

[25] *Id.*

[26] *Id.*

3. Facilitating Researchers' Access to De-Identification Tools Through Administrative Data Research Networks.

Relevance: Topics 6, 8, and 9.

Finally, a national strategy should advance PETs by further encouraging government agencies to implement Administrative Data Research Networks (ADRNs). De-identification tools are sought by a diverse array of organizations across many sectors of the economy. Despite this widespread interest, many organizations cannot utilize de-identification tools due to the significant amount of expertise and resources required to adopt these technologies. Implementation and resource barriers can hinder beneficial activity, such as improvements to municipal services through open data initiatives.[27] Researchers that cannot obtain and deftly operate de-identification tools may encounter hurdles to accessing administrative data, or information held by organizations.[28] Concerns about sharing data with researchers[29] can frustrate innovation and evidence-based policymaking.

- **Recommendation:** Encourage the establishment of Administrative Data Research Networks (ADRNs) that offer de-identification tools to facilitate researcher access to data in a protective manner.

A national strategy to advance PETs should further encourage government agencies to implement Administrative Data Research Networks (ADRNs). ADRNs are networks of Administrative Data Research Facilities (ADRFs), which are intermediary institutions that offer secure computing platforms for researchers to access data held by other organizations, such as government agencies.[30] ADRNs would support the growth of PETs by: establishing the appropriate de-identification standards needed to facilitate the

---

[27] Kelsey Finch, *City of Seattle Open Data Risk Assessment*, Future of Privacy Forum, 7, (2018), , Accessed June 27, 2022, https://fpf.org/wp-content/uploads/2018/01/FPF -Open-Data-Risk-Assessment -for-City-of-Seattle.pdf, ("Tremendous benefits in healthcare, education, housing, transportation, criminal justice, and public safety are already being realized as richer and more timely datasets are made available to the public. Open data can unite the power of city and private sector abilities to improve community health and lifestyles, from bikeshare systems and commercial apps harnessing transit data to community advocates shining the light on ineffective or discriminatory practices through policing and criminal justice data.").

[28] Daniel Goroff, Jules Polonetsky, and Omer Tene, *Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data*, 675 Annals Am. Acad. Pol. & Soc. Sci., 49 (defining administrative data as data that one organization collected that "researchers access . . . for a purpose different from the one for which the data were originally collected.").

[29] *Id.* at 48, ("[T]he ability of researchers to access significant government datasets is often limited by a range of concerns, in large part consisting of privacy and security objections.").

[30] Coleridge Initiative, *Administrative Data Research Facility*, Accessed July 6, 2022, https://coleridgeinitiative.org/adrf/.

sharing of administrative data with researchers, demonstrating the value of investment in PETs; and creating a market for nascent privacy engineering.

More specifically, ADRFs can create procedures to improve accuracy, efficacy and privacy at the data input, computation, and output stages.[31] These facilities would also institute accountability measures for auditing and monitoring compliance with data-sharing rules.[32] ADRNs would function as forums where individual ADRFs share best practices and identity standards that apply across industry sectors. For example, ADRFs could create working groups on topics such as data security, private and proprietary data protections, and more.[33] To deter misbehavior. ADRNs could rescind a researcher or ADRF's status, privileges, and data access.[34]

Thank you for this opportunity to provide input on the specific actions that could advance the adoption of privacy-enhancing technologies (PETs) in a responsible manner. We welcome any further opportunities to provide resources or information to assist in this important effort. For more information or to clarify any information provided here, please contact Daniel Berrick at dberrick@fpf.org.

Sincerely,

Daniel Berrick
Policy Counsel, Future of Privacy Forum

Jules Polonetsky
CEO, Future of Privacy Forum

Limor Shmerling Magazanik
Managing Director, Israel Tech Policy Institute

Future of Privacy Forum

1350 Eye Street. NW, Suite 350

Washington, DC, 20005

info@fpf.org

[31] Daniel Goroff et al., *supra* note 28, at 61.
[32] *Id.* at 60.
[33] *Id.*
[34] *Id.*