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

## Visa Inc

**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.

# U.S. Office of Science and Technology Policy (OSTP)

# Request for Information on Advancing Privacy-Enhancing Technologies

Notice Published on the Federal Register on June 9, 2022

**Visa Inc.'s Response to OSTP's RFI on Advancing Privacy-Enhancing Technologies (PETs)**

**Submitted by Visa's Global Privacy Office and Global Strategic Initiatives Teams**
July 8, 2022

Visa welcomes the opportunity to provide input on privacy-enhancing technologies ("PETs") and their emerging role in data-sharing and collaborative analytics. We look forward to continuing this important dialogue as an industry stakeholder.

If you would like to discuss any of our responses in greater detail, please contact the Visa Chief Privacy Officer, Leigh Feldman, or Visa Global Privacy Counsel, Sunny Seon Kang.

Please find Visa's comments below.

## 1. Specific research opportunities to advance PETs:

Hackathons, tech sprints, and regulatory sandboxes provide opportunities for cross-functional stakeholders to collaborate on a problem statement and navigate solutions through the participants' diverse expertise and perspectives. The value of these workshops is in welcoming multidisciplinary approaches to a common challenge, such as applying a technological solution to a traditionally legal and regulatory problem.[1] The role of hackathons in validating modern PETs and associated cryptographic methods has been demonstrated as early as 2006 with the Netflix Prize Dataset de-identification challenge, which tested the robustness of anonymization techniques against adversarial attacks.[2]

PETs are currently at a juncture of evolving from academic research to practical and scalable application. Research by the Financial Action Task Force identified one of the main barriers to PETs adoption as the lack of certainty on compliance standards.[3] Therefore, the development of PETs would benefit from

[1] For example, the U.S. Consumer Financial Protection Bureau (CFPB) published a request for information in 2019 on utilizing "Tech Sprints as a means to encourage regulatory innovation and collaborate with stakeholders in developing viable solutions to regulatory compliance challenges" and cited the UK Financial Conduct Authority's hackathon they hosted on PETs solutions for anti-money laundering and financial crime challenges. See at, https://www.federalregister.gov/documents/2019/09/18/2019-20201/request-for-information-regarding-tech-sprints.

[2] Narayanan and Shmatikov, *How To Break Anonymity of the Netflix Prize Dataset*, Cornell University Database (November 2007): https://arxiv.org/abs/cs/0610105

[3] Financial Action Task Force (FATF), *STOCKTAKE ON DATA POOLING, COLLABORATIVE ANALYTICS AND DATA PROTECTION* (July 2021): https://www.fatf-gafi.org/media/fatf/documents/Stocktake-Datapooling-Collaborative-Analytics.pdf

examining their proof of concept in hackathons which focus on a real-life use cases, often through regulatory supervision and partnership.[4]

As the White House Office of Science and Technology Policy ("OSTP"), U.S. National Science Foundation, and U.S. National Institute of Standards and Technology ("NIST") jointly work with the UK government to develop PETs challenges in the coming year,[5] we believe it would be beneficial to encourage industry collaboration with academic researchers and universities in the challenges, and to work towards an outcome that furthers technical guidance and best practices for privacy-preserving analytics.

### 2. Specific technical aspects or limitations of PETs:

PETs collectively refer to a variety of computing techniques, including but not limited to: differential privacy, use of synthetic data, federated learning, homomorphic encryption, and secure multi-party computation. Although many of these techniques have a long history of academic research and development, their deployment in the enterprise environment is still relatively nascent and exploratory in certain sectors.

It is important to note that each privacy-preserving technique entails constraints and tradeoffs. Certain methods of de-identification can diminish the usability and accuracy of data. For example, differential privacy injects noise to protect data subjects from identifiability, but doing so decreases the accuracy of analytics done with that data.[6] Additionally, computational overheads associated with cryptographic methods often cause delays in processing, limiting their application to more complex machine learning models such as decision trees or neural nets.[7]

Some of the constraints listed above have been mitigated by combining two or more types of PETs, such as federated learning with differential privacy, secure multi-party computation and homomorphic encryption, and so forth.[8]

### 3. Existing barriers *related to PETs adoption; how regulatory frameworks may address them:*

A technical understanding of PETs should underpin the policy framework. This would ensure that regulatory guidance on PETs is neither quickly outpaced by innovation nor overly prescriptive such that it would inhibit new technical approaches.

Organizations interested in exploring PETs as an additional safeguard would benefit from regulatory guidance which clarifies compliance standards (i.e. in defining what constitutes anonymization versus pseudonymization) while also providing flexibility on the technical approach to achieve that standard.

[5] https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/

[6] Bagdasaryan et al, *Differential Privacy Has Disparate Impact on Model Accuracy*, 33rd Conference on Neural Information Processing Systems (NeurIPS 2019): https://proceedings.neurips.cc/paper/2019/file/fc0de4e0396fff257ea362983c2dda5a-Paper.pdf.

[7] Damgard et al, *Perfectly Secure Multiparty Computation and the Computational Overhead of Cryptography*, International Association for Cryptologic Research (2010): https://link.springer.com/content/pdf/10.1007/978-3-642-13190-5_23.pdf

[8] Civil society groups such as Future of Privacy Forum and the International Association of Privacy Professionals have published on market and regulatory frameworks propelling PETs. See, *Future of Privacy Forum, Privacy Tech's Third Generation A Review of the Emerging Privacy Tech Sector* (June 2021): https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf

Regulatory clarity on utilizing PETs would accelerate PETs adoption as organizations would better understand their obligations when approaching a new way of computing or sharing data.

4. *Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs:*

The advancement of PETs is particularly important to privacy-preserving machine learning and network analysis in investigating financial crimes. The emerging role of PETs in the financial sector has been examined by the World Economic Forum[9] and the Royal United Services Institute.[10] The United Nations has published a white paper on privacy-preserving computation techniques which examines their applicability to statistics and model development.[11]

5. Best practices that are helpful for PETs adoption:

Data privacy and security through PETs can achieve greater data accountability and informational autonomy for data subjects. Privacy-by-design, especially through PETs, should be emphasized as a critical step to proactively mitigating privacy risks.

Technological advances in privacy-preserving tools are creating an opportunity for organizations to work towards preventing, rather than reacting, to data-related harms. Thus, the focus of best practices should be reframed from avoiding consumer harms to championing consumer empowerment through de-identification and PETs.

[9] World Economic Forum, *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value* (September 2019): https://www3.weforum.org/docs/WEF_Next_Gen_Data_Sharing_Financial_Services.pdf

[10] RUSI, *Future of Financial Intelligence Sharing (FFIS) Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime* (January 2021): https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf

[11] United Nations, *UN Handbook on Privacy-Preserving Computation Techniques*: https://unstats.un.org/bigdata/task-teams/privacy/UN%20Handbook%20for%20Privacy-Preserving%20Techniques.pdf