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

Mastercard

July 8, 2022

By Electronic Mail to: PETS-RFI@nitrd.gov

Re: **RFI Response: Privacy-Enhancing Technologies**

Respondent: Caroline Louveaux, Chief Privacy Officer at Mastercard (Respondent Type: Industry)

Mastercard welcomes the opportunity to provide comments in response to the White House Office of Science and Technology Policy's ("OSTP") **request for information ("RFI") on Advancing Privacy-Enhancing Technologies**. As a technology company in the financial services space, we are exploring a variety of privacy-enhancing technologies ("PETs") in line with the data practices outlined in our Global Data Responsibility Imperative.[1] In our comments, we provide background on Mastercard's work in the PET space and outline some of the unique challenges that organizations face when deploying PETs. Our comments will provide examples of areas that could benefit from enhanced PET adoption and recommendations that we believe would advance the development and adoption of PETs in a way that offers high levels of protection for individuals, while also enabling data-driven innovation. In particular, we encourage OSTP and other regulators to promote PET adoption, to clarify that a dataset subject to appropriate PETs is not subject to data protection laws while still holding companies accountable for their use of PETs, and to actively monitor the field in the near term as technology continues to evolve. For ease of reference, we note the corresponding RFI topic numbers to which each section of our response pertains.

Exploring Opportunities for PETs (RFI topics 1, 3, 10)

At Mastercard, we have dedicated resources across a variety of teams to explore PETs including synthetic data, differential privacy, and transformation techniques with risk scoring for our data insights capabilities. Our research has demonstrated that while each solution has its own pros and cons and appropriate use cases, all of these technologies have a positive contribution to make to the field of privacy-compliant data analytics. We strongly support adoption of these tools to enhance individual privacy while enabling data innovation - both to power new products and services and help solve some of society's most pressing challenges.

Our exploration of these technologies is driven by a strong privacy culture combined with our technology mission. Bringing these two elements together has resulted in the development of a suite of new products and services. Our Data & Services team, for example, drives efficiency and value for our customers (from small businesses to large enterprises) and empowers them to solve problems with powerful analytics tools. As another example, our Cyber &

[1] Our Global Data Responsibility Imperative is a vision of how Mastercard believes data can be leveraged in a responsible and secure way to drive relevant benefits for individuals and society. It posits that individuals hold certain data rights and explains why data responsibility is a business and moral imperative. It proposes a model framework for how organizations could approach personal information and lays out principles to guide organizations' data practices, as well as characterizing the critical role data has in driving inclusive economic growth across the globe.

Intelligence teams help prevent fraud, financial crime, and cyber-attacks with sophisticated data-based tools that can spot individual and systemic level risks without compromising any personal information.

We are also committed to the use of data analytics to aid in humanitarianism, inclusive growth, pressing societal issues such as climate change, and global health crises. We work across industry and with private and public partners alike on projects for the public good. Mastercard's Center for Inclusive Growth has collaborated with governments, universities, and non-profits on a number of projects to responsibly deliver data-driven insights that enable a better understanding of inclusive growth around the world. For example, insights based on Mastercard's anonymized and aggregated spending data have helped with challenges faced by low-income communities in Chicago by offering a much more detailed, nearly real-time glimpse into not just what communities spend on, but where they spend, aiding public- and private-sector entities to ensure investments meet local needs and lower the cost of living. Our data insights have also been valuable following natural disasters and in recovering from the pandemic's impact on the global economy. We also recognize that synthetic data tools can support the advancement of inclusive growth and humanitarian objectives.

Other potential PET use cases include training machine learning models with synthetic data, which minimizes privacy risks while maximizing responsible innovation and healthy competition. PETs also enable new solutions to various problems through privacy protecting data combinations, where parties can share insights gained from multiple datasets without having to share the underlying data. For example, in the financial services industry the wide generation of synthetic data could help coalitions of companies and regulators to identify systemic risks or threats.

All of these uses of data will benefit from the evolution of tools and techniques in the PET space, provided that regulators and companies partner to support their development, acceptance, testing, and continued improvement. We believe that regulators should strongly endorse PETs, and clearly articulate that when the risk of re-identification of a dataset is sufficiently remote, the use of PETs should exclude the applicability of data protection law to a given dataset.

Regulatory ambiguity can have negative real-world consequences for innovation and social impact by disincentivizing companies and discouraging market entry. As examples, in markets where regulatory ambiguity increases risk and the cost of compliance for businesses, products that aid small businesses may take longer to launch, or tools for inclusive growth that require data to make decisions may be prioritized in other markets where risks and barriers to entry are lower. Certainty around privacy regulation, and the use of PETs in particular, will be fundamental in the coming years for innovation efficiency.

Reviewing the Challenges of Deploying PETs (RFI topics 2, 4, 5, 7, 9)

To fully appreciate the need for regulator endorsement of PETs, it is important to understand that organizations are naturally hesitant to enter a new field without a clear understanding of the technology, cost, and anticipated regulatory environment. The adoption of PETs within a large organization will require significant capital investment, potentially measured in the millions of dollars depending on the size and scale of a company.

At a minimum, deploying a PET will require financial resources to purchase or license the requisite software and hardware, and investments in personnel with a variety of skillsets. A successful deployment of a *single* PET may require software engineers, hardware engineers, corporate security specialists, privacy lawyers, privacy engineers,

project managers, data analysts, data modelers, database administrators, data strategy experts, and "red teams" to test, simply to make a PET *available* within an organization's environments – before the PET is even applied responsibly to a product, service, or dataset. Testing and tuning a variety of different PETs further increases the demand on resources.

The complex and fragmented data protection regulatory landscape, both globally and within the United States, creates headwinds against PET adoption. Varied anonymization and/or deidentification thresholds under applicable state and federal laws create challenges for responsible industry players who seek to lead the way in unlocking the benefits of PETs. As we describe below, clear regulatory endorsement of PET development, acceptance, testing, and continued improvement will help mitigate some of these challenges.

Providing Regulator Endorsement to Drive Industry Adoption of PETs (RFI topics 5, 6, 8, 9, 10)

While some companies will take a pioneering role and invest in the PET space, the majority of them will take a wait-and-see approach which will slow innovation. To minimize this risk and remain competitive on the global stage, regulators should make clear that data subjected to appropriate PETs will fall outside the scope of data protection law, provided that the risk of linkage or re-identification in the dataset is within reasonable risk thresholds supported by research.

In addition, regulators should provide reasonable flexibility in the selection of various technologies until the field matures. Although a dominant technology is likely to emerge, we anticipate that forms of synthetic data, differential privacy, and transformation techniques with risk scoring will each play a role depending on use case (homomorphic encryption and secure multiparty computation will also add to the PET space depending on the use case, such as data sharing). For example, there are multiple techniques for generating synthetic data and different risks with each approach; while no single technique has yet been identified as the best model, regulators should continue to monitor the research and provide appropriate guidance on synthetic data as this field develops.[2] Anonymization by an independent third party may also be a solution or requirement in some cases. Existing technologies that were once computationally intensive will become a reality with newer computing resources. In each case, however, regulators can and should rely on reasonable re-identification risk thresholds to ensure that a technology maintains privacy, while endorsing the PET space in general.

We also highlight that use cases vary between companies and industries, and different use cases will have varying risks of re-identification and different "release models" (internal use only, external release of a dataset, or external release in aggregate form, as examples). In the financial services space, companies often find significant value in producing reporting that is aggregated, e.g., at the city level or, in some cases, a neighbourhood level with sufficient population sizes. The re-identification risk in such a use case is lower than what may be required when publicly releasing or allowing third parties to carry out analytics on granular data. Similarly, the risk levels with financial

[2] With regard to synthetic data in particular, it can be difficult to identify the age of a synthetic dataset, so markers should be added to the data to make this easy. In addition, only the original creator of a synthetic dataset will know how statistically close to the original dataset it is. If synthetic data is to be sold to or re-used by a third party, there should be a standard approach to describing the veracity of the synthetic dataset, without disclosing information that could reduce the privacy protections. These are areas where best practices are not yet defined but should be appropriately standardized.

transaction data may differ from health data or social media data that, by the nature of data elements included in a dataset, may be more identifiable or entail different privacy interests for individuals.

Nevertheless, as consumer-supporting industries seek to meet consumer needs in a variety of ways, a sector-specific approach to data would create uncertainty and inconsistency in how industries apply PETs for data analytics. For those reasons, companies should have internal flexibility to select risk thresholds for re-identification across a spectrum of identifiability and privacy risk, within reasonable constraints supported by research. Regulators could consider issuing grants to fund academic research or conduct meta-analysis in these areas. We also see that academic publications, patent applications, and commercial research are beginning to emerge that demonstrate the application of mathematical discipline to determining the risk of re-identification. Such research could inform the flexibility and guardrails given by regulators to companies using applicable technologies.

To drive adoption, regulators should also make clear that the act of applying PETs to identifiable information does *not* require additional or separate consent of an individual and falls outside of consent frameworks imposed by data protection law. PETs are intended to preserve and enhance privacy, and companies should be incentivized by removing uncertainty around legal requirements or withdrawing additional barriers. Similarly, it should be clear that companies may outsource PET functionality to vendors, as vendors are likely to have advanced capabilities backed by research and publications, and advanced technology.

Finally, due to the privacy-preserving nature of data processed by PETs and the inability to re-identify a dataset, it should be made clear that companies do not need to destroy an original dataset in order to comply with data protection laws, although it should be kept separate and under strict access controls. Companies may have separate uses and a separate legal basis for the personal data contained in an original dataset, such as to enable a primary business purpose or facilitate a transaction at the direction of a consumer, while data processed by PETs could be used for aggregated analytics or "data for good" projects.

Holding Organizations Accountable While Supporting Innovation of PETs (RFI topics 2, 7, 8, 10)

In line with privacy principles around accountability, and in exchange for regulator endorsement of PETs, regulators should hold companies accountable for their use of PETs. As with other technologies and uses of data, companies must deploy technical and organizational measures to demonstrate that their use of PETs in each context is appropriate. This could include documentation on why a PET was selected for a particular use case, the data elements involved, the type and nature of the processing and analytics, the outputs and levels of aggregation, the release model, and the selected risk threshold (or results of a motivated intruder analysis). These measures would be combined with records of processing, data protection impact assessments, and other normal recordkeeping as part of a robust privacy program.

Regulators should also encourage vendors in the PET space to consider the "explainability" of their PETs from the earliest stages of development, just as privacy by design requires engagement of privacy principles from day one of product development. Vendors in this space could build, for example, dashboards or reporting capabilities with appropriate explanations of how a tool was deployed, how risks of re-identification or singling out were minimized, and which risk thresholds were used based on the intended use case, release model, and aggregation level of the output. Regulators might also consider developing an industry code of conduct that provides guidance on how

companies can promote their use of PETs to consumers in a user-friendly and accurate manner, based on the controls and technical and organizational measures that they have in place.

Companies benefitting from the use of PETs should also be required to demonstrate they have made appropriate investments in their controls and auditing, which may include the retention of privacy counsel, privacy engineers, and auditors with expertise in the area.

Keeping Pace with Technological Innovation and Developments in the Law (RFI topics 1, 4)

Finally, we encourage regulators to stay actively involved in the conversation surrounding PETs, especially in the next few years as rapid advancements in the technology are expected. Academic and commercial research may shift thinking toward one technology or demonstrate that certain use cases are lower or higher risk than others. Continued regulator engagement in this area will encourage the rapid pace of innovation with a focus on privacy of the individual.

We are available to answer questions that OSTP may have regarding our comments, and we would welcome an opportunity to further discuss this topic with you at your best convenience.