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

The Ethical Tech Project

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.

July 8th, 2022
To: Office of Science and Technology Policy
From: The Ethical Tech Project
Re: **RFI Response: Advancing Privacy-Enhancing Technologies**

To Whom It May Concern:

The Ethical Tech Project is an advocacy group that works across the worlds of business, academia, and government to build ethical data and privacy practices in organizations of all types and sizes.

Our vision is a future where technology supports human flourishing, where everyday consumers' rights are aligned with business practices such that data can build better products, services, and experiences while still respecting the dignity of consumers and citizens.

Privacy-Enhancing Technologies (PETs) are essential to achieving this vision and bridging the gap between regulations and standards set by policymakers, legal and compliance experts, engineers, product managers, and technologists on the ground building.

PETs will not see broad adoption unless regulators work in concert with technologists that build, maintain and own the systems responsible for enforcing the regulations. Whether it is a business, a government or state actor, or an NGO, the bottom line of the privacy problem is that someone somewhere is engineering a system around data that must have privacy-by-design. We believe that the only way to ensure this happens within the context of our market system is through the mechanism of voluntary Privacy Standards that achieve a critical level of adoption. We look forward to offering the details in the following responses to your RFI on Advancing Privacy-Enhancing Technologies.

Sincerely,

The Ethical Tech Project

Responses

1. Specific research opportunities to advance PETs

No comment.

2. Specific technical aspects or limitations of PETs

PETs do not exist in a silo: they must be part and parcel of a concerted architecture that includes established tech already broadly in use today in order to accomplish the specific demands of a privacy-by-demand system. At the Ethical Tech Project, we have identified **five requirements** for data users (businesses and other organizations that make use of individual data) to respect the permissions of data owners (individual citizens that are the originators of personal data).

Permission – the granular conditions for the use of every datum for every user and every purpose – is fundamental to privacy and the notions of Data Control (the opportunity for individual data owners to have the choice over what happens to the data that originates with them) and Data Dignity (the concept that data owners must have negotiation power over the use of their data, enabled by Data Control). The technical aspects of PETs must possess *all five* of these requirements in order to comprehensively respect permission:

A. **Purpose** - Make purpose a 'first-class citizen' in the consideration set for processing data through systems to **declare**, **enforce**, and **audit** permissions.
B. **Control** - Afford data owners the means to control their data through the **granting**, **revoking**, and **enforcing** of permissions and the ability to execute data **control operations**.
C. **Recognition** - Make explicit the **recognition** and identification of all entities participating in the data transaction with associated **registration**, **verification**, and **revocation** procedures.
D. **Transmission** - Support transmission of instructions and permissions from end to end across data supply chains through **subscription** and **broadcasting** procedures across the chain and **auditing** and **enforcement** procedures within each link.
E. **Rectification** - Take remedial steps to **rectify** instances when permissions or instructions are not respected and **monitor** and **alert** for such instances.

How do these requirements translate into a technical architecture? At a technical level, privacy-by-design is in practice applied through a robust system across Apps, Services, and an organization's data stack in order to protect the individual's privacy rights (please refer to our "Privacy Stack" diagram in the Appendix). The components of the "Privacy Stack" exist in at the application and service levels, and comprise existing off-the-shelf solutions such as Identity Management that must work in concert. Our delineation of those components are:

- **Apps**
    - Data Risk Management
    - Responsive Regulatory Compliance
    - Automated Subject Rights Fulfillment
    - Consent and Preference Management
- **Services**
    - Policies for the Access and Use of Data
    - Identity and Entity Management
    - Granular Data Permissioning
    - Privacy CMS
    - Data Discovery and Classification
    - Access Control
    - Data Control
    - Integrations

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

No comment.

4. Specific regulations or authorities that could be used, modified, or introduced to advance PETs

No comment.

5. Specific laws that could be used, modified, or introduced to advance PETs

No comment.

6. Specific mechanisms, not covered above, that could be used, modified, or introduced to advance PETs

We are advocates for standards, coupled with reference architectuers, as a mechanism to make PETs easily adaptable. In other areas where data is sensitive or regulated, standards such as PCI-DSS, SOC 2, and others have achieved broad adoption and made it simple to understand how compliance may be reached. Even if achieving compliance is arduous, standards provide a template to snap to and give industry a space to innovate around a shared understanding and concrete expectations of what to build.

Privacy Standards are already on the market, but they face three challenges when it comes to adoption by engineers building products:

1. Deriving **technical specifications from otherwise non-technical requirements** is difficult - better standards must be flexible while still offering engineers a firm pattern to build around. Coupling standards with example reference architectures will support adoption and adherance from technologists.
2. Evaluation of various PETs on the market comes with a **high level of friction and cost of doing business** that current privacy standards do not come close to alleviating - a standard by engineers for engineers with the blessing of policy leaders would reduce cost of doing business by removing and fastracking technology evaluations.
3. **Incentives are not currently aligned to motivate market forces** to drive the behavioral change that PETs aim for - PETs fundamentally are the tools necessary to advance respect for permission, Data Control, and Data Dignity, but as tools they will not be adopted without stronger incentives that a uniform standards-based ecosystem creates (see here for reference).

Surmounting these challenges is essential to advance the mechanism of standards and drive the adoption of PETs broadly.

7. Risks related to PETs adoption

As technologists seeking to bridge the gap between the work of law and policy and the world of those on the ground building products, we see an existential risk to PETs adoption are laws made in a silo without the input of engineers who then have to implement those laws. Laws must be accompanied by standards, frameworks, and patterns for engineers to quickly turn policies into action. These can be created by government, academia, nonprofits, advocacy groups, or for-profit enterprise, but the bullhorn of policymakers can help ensure awareness, adoption, and eventual success.

8. Existing best practices that are helpful for PETs adoption

Standards and reference architectures for engineers are essential to PETs adoption. Engineers are fundamentally problem solvers. When they see a problem, they seek a solution, and every engineer knows there are multiple ways to get the job done with accompanying trade-offs in terms of risk, time, and resource. Every engineer thus seeks out established patterns, frameworks, and solutions that have worked for others before them and can be adapted for the product they are building. We need to see this best practice - which has achieved broad adoption in areas such as security - applied to the privacy space. Therefore, there needs to be disseminated everywhere patterns, designs, reference architectures, and standards for how to implement PETs across different use cases and industries. A good place to start is the “privacy stack” architecture being generated by The Ethical Tech Project.

9. Existing barriers, not covered above, to PETs adoption

To detail our third challenge articulated in our response to #6, PETs adoption requires incentives. Incentives can be carrots, or they can be sticks. Privacy regulations such as GDPR or CPRA are sticks driving adoption. Conversely, there aren't any carrots incentivizing adoption at the same scale as privacy law regulation. This does not mean that positive incentives aren't possible: there are many instances of industry self-regulation that have used the positive incentives of a standard to reward those that adopt. A barrier today is that there is no positive incentive framework or standard for privacy that has achieved critical mass in terms of awareness and adoption. This is an opportunity for the government to step in and advocate for such a standard with positive incentives.

10. Other information that is relevant to the adoption of PETs

No comment.

Appendix

Privacy Stack Diagram