

## **Request for Information (RFI) on Advancing Privacy Enhancing Technologies**

**Prifina 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.



**Response to the notice of request for information on  
advancing privacy-enhancing technologies  
(87 FR 35250, Doc. Nr. 2022-12432)**

*To*

*Office of Science and  
Technology Policy (OSTP)*

*July 8, 2022*

*On behalf of*

*Prifina, Inc.*

*Address*

1250 31st Avenue  
San Francisco, CA  
94122 USA

*Email*

*policy@prifina.com*

To whom it may concern,

Prifina Inc. is pleased to have the opportunity to respond to the request for information on advancing privacy-enhancing technologies. We are grateful for making it possible for various interested parties to express their views on this highly significant and timely area of innovation.

Prifina appreciates the work that the Office of Science and Technology is doing. The privacy-enhancing technologies have been developed for quite a while, and we are reaching the tipping point when such PETs will be available not only for legacy technology giants but also to benefit individual consumers.

The lack of a uniform data and privacy framework on the federal level is only one factor that contributes to the lack of certainty about how companies handle user-generated data. In our response, we propose that privacy-enhancing technologies in general, and the user-held data model in particular, provide a viable long-term solution to ensuring that user-generated data is utilized responsibly and ethically. Without major regulatory interventions, the user-held data model helps achieve many policy objectives - individual autonomy, data minimization, lawful and transparent data usage by third parties, data portability, and interoperability. We also propose steps that the executive branch could take to advance the adoption of PETs.

We admire that the Office of Science and Technology Policy has taken a firm stance to advance privacy-enhancing technologies and protect consumers' data privacy rights while maintaining the fair and efficient functioning of the digital market.

Should you have any questions, please do not hesitate to contact us.

Sincerely yours,

Markus Lampinen, Jouko Ahvenainen and Paul Jurcys

## About Prifina

Prifina is a VC-backed company building a new data architecture where individuals own and control their data ("user-held data model"). This type of data architecture enables new use cases and personal applications to be designed and built on top of user-held data.

Prifina's mission is to create an environment where individual users can get daily value from their personal data and where developers can build applications that help generate value from such data. We believe that personal and user-generated data can help individuals live healthier and happier lives and that personal data has a long-term value to individuals.

The starting premise of Prifina's user-held data model is the ability of each individual to collect their data from various data sources (wearable devices such as smartwatches or smart rings, online accounts, paper documents, etc.) into their "personal data clouds." Every personal data cloud is supported by a dynamic software layer that cleans and organizes the data format and makes data efficiently utilizable by apps. By default, only the user can access data in the personal data cloud; third parties cannot access any data unless the user gives prior express authorization. Prifina's user-held data model is user-centric: the user has exclusive and ultimate agency and control over the data held in the personal data cloud. Furthermore, in the user-held data environment, individuals are also legal owners of their user-held data (i.e., the data in each user's personal data cloud).

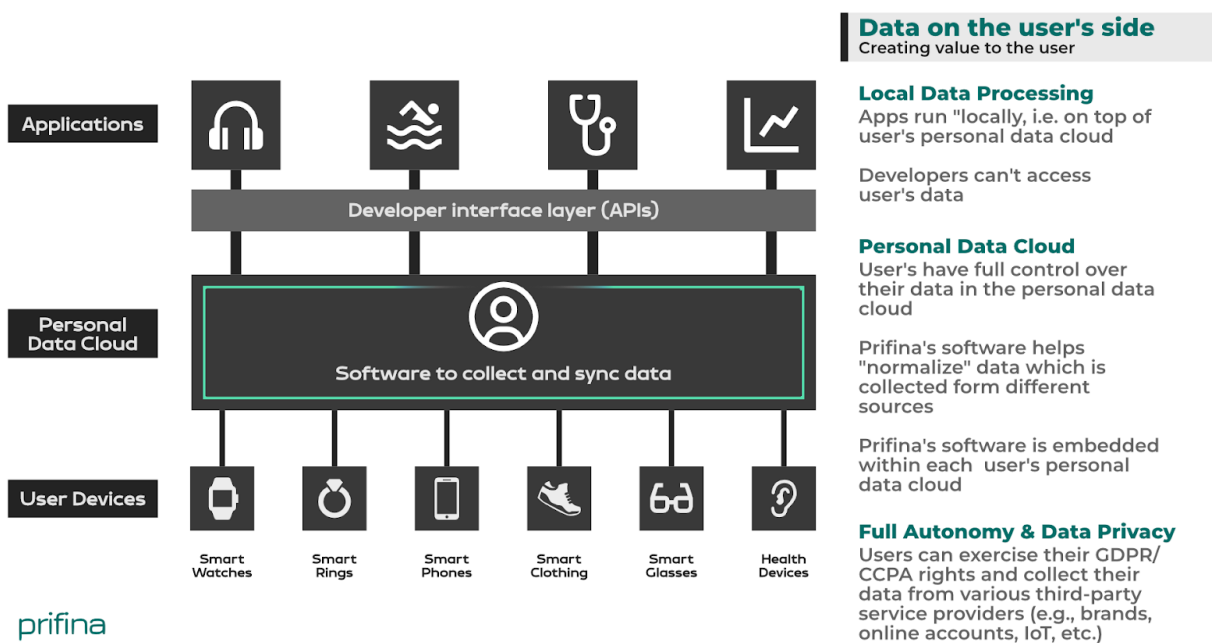
The "user-held data model" opens new opportunities for generating value from personal and user-generated data. Prifina is developing an intelligent data layer that helps normalize the data that is collected in users' personal data clouds. Using Prifina's resources and tools, developers can easily add new data sources and build new applications that run on top of user-held data (i.e., apps run locally in each user's personal data cloud). As a result, the value from user-held data is captured on the user's side.

The user-held data model has two important implications: First, users can better understand the depth and breadth of their data and have full ownership and control over it. Secondly, the user-held data model separates data from the applications.

This user-centric, user-held data approach is in line with the general principles of data privacy laws: that data is being used only with the user's prior consent, data minimization (here, the service provider does not have to hold any data on its own servers), transparency, purpose limitation (that data is used only for clearly defined purpose), data security and data portability.

The user-held data model opens new perspectives concerning the portability of personal and user-generated data. Rather than data being "ported" from service provider A to service providers B and C, service providers come to every user through new applications that run in users' personal data clouds. This means that service providers can better understand their potential customers and avoid huge risks associated with holding customer data on their own servers.

The user-held data model offers compelling technological architecture and multi-stakeholder incentives to realize the Commission's vision to build a new data ecosystem based on human-centric data values. This data model inspires people to think about "activating" data to unlock the value from data for individuals and developers/businesses and open the gates to building user-centric data apps for "smart citizens." Furthermore, the user-centric data model will likely become one of the possible technological solutions for utilizing user-generated data for research and reaching sustainability goals.



## 1. Specific research opportunities to advance PETs

The user-held data model offers opportunities to make more user-centric data services. It means that the service can include richer data on an individual, combine data from many sources and then provide tailored services for the individual. Adopting such an approach to data requires new models to analyze data and train Machine Learning models. The user-held data model offers many new research opportunities, from technology to data science and business models.

Building on a user-specific data set, there is the opportunity to research individual baselines and establish different ways of preventing and handling deviations. For example, establishing a baseline for an individual's sleep patterns can help prevent deviations such as sleep disruptions, circadian rhythm disruptions, handling shift work, and many other situations in everyday life based on personalized data sets.

However, centralized (or "siloed") data models prevail today. Such centralized data models contain data sets that are very rich on an *aggregate* level, but narrow as it comes to individuals. In practice, centralized data models mean that while there may be many individual data points about the specific question, such as sleep data, the other factors, such as contextual data, behavior, activities, interests, etc. are lost from that aggregated data set. This is so because the privacy concerns and the size limitations of a centralized data set constrain what is possible to collect.

An individualized dataset, such as the one proposed by Prifina, unlocks this limitation because the individual's dataset can be incredibly rich and deep.

## 2. Specific technical aspects or limitations of PETs

The user-held data model is very different from the traditional big data approach. The user-held data model means changes and improvements for the technology, data models, analytics, and applications. For example:

1. Data storage and cloud solutions must enable individuals to store their own data and run applications so that the data never leaves the user's environment.
2. Analytics is based on rich data on an individual rather than sparse data from many individuals. This requires new types of algorithms and models to analyze data and teach machine learning models (e.g., federated learning type models).

3. If an individual wants to share some data, new cryptographic models are needed to limit the use of the data only for the purposes it was shared.
4. In many cases, bringing the processing near an individual would be better. This requires an edge computing type of technology and models to store and process the data.

From a technical perspective, the main challenges in building the new user-centric data ecosystem relate to the fact that (i) data is locked in silos and that there and (ii) there are no common/unified data layers. These two factors are among the most challenging obstacles that need to be overcome to facilitate the flow of data.

#### Further references:

- **Paulius Jurcys, et al., 'My Data, My Terms: A Proposal for Personal Data Use Licenses'**, *Harvard Journal of Law and Technology Digest* (2020), available at: <https://jolt.law.harvard.edu/digest/my-data-my-terms>

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

**Health and well-being** are becoming more important all the time for individuals and societies. Digital healthcare and wellbeing services offer significant opportunities to improve personal health and well-being and make healthcare more cost-effective. However, privacy and data protection are crucial with health data and health services. Responsible use of personal health data and wellness data has become even more critical after the Supreme Court's ruling in *Dobbs*.

The user-held data model with personal applications that can be run on a person's own data offers significant new opportunities to improve health and wellbeing services. At the same time, it is possible to get more data from individuals, for example, wearable data that already now has information on heart rate, exercising, and sleeping. New sensors enable measuring e.g., blood pressure, blood glucose, lactate, or inflammations. With the user-held data model, individuals can also share data with healthcare providers, making it easy for individuals to use those services they wish and always share necessary data.

The user-held data model can be adopted in various other sectors and verticals: IoT, geo-location and mobility, financial, insurance, smart cities, GovTech, etc. The key objective here is putting the individual in the middle of digital interactions, empowering them to *opt-in* to various services (rather than placing a hefty burden

on individuals to opt-out), and, most importantly, making sure that the value from user-generated data is captured on the user side.

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

The impact of currently existing laws and regulations on the federal and state levels is relatively limited. Practically, individuals have very little control over how organizations access and use individuals' personal and user-generated data. While the adoption of the federal privacy act is pending, government agencies could take steps to adopt "soft" measures that could facilitate a more transparent and responsible use of personal and user-generated data (see section 6 below).

##### **Clarification of data access/ownership rights.**

From a legal and technical perspective, it is important to ascertain that individuals have unlimited access to the data about themselves regardless of where it is held.

##### **The Use of Biometric Data.**

The emergence of virtual work and play environments (including "metaverses") raises many questions about the utility of user-generated and biometric data. The user-held data model could prove helpful because it allows individuals to control their avatar data. This, of course, raises various issues related to data portability and interoperability.

##### **The use of non-clinical data in health care.**

As health-monitoring sensors become widespread, various questions emerge about the utility of such user-generated wearable data in health care. Currently, wearable device makers collect vast amounts of user-generated data, which is locked in the walled gardens of such devices. In the future, it would be desirable if such data could be unlocked and made available to individual users who generate such data. Homomorphic encryption could prove to be especially useful in this context.

##### **Further references:**

- **Paulius Jurcys et al., 'Ownership of User-Held Data: Why Property Law is the Right Approach', *Harvard Journal of Law and Technology Digest* (2021), available at: [jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach](http://jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach)**

- **Jouko Ahvenainen, 'The metaverse is coming for your biometric and health data'** available at: [medium.com/prifina/the-metaverse-is-coming-for-your-biometric-and-health-data-1d185a93519c](https://medium.com/prifina/the-metaverse-is-coming-for-your-biometric-and-health-data-1d185a93519c)
- **Marcelo Corrales Compagnucci, et al., 'Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector?', 3(4) European Pharmaceutical Law Review (2019) available at: <https://eplr.lexxion.eu/article/EPLR/2019/4/5>**

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

### **Federal privacy law.**

It would be most desirable if the US Congress could adopt a federal privacy act that is based on user-centric principles (data minimization, data portability, data interoperability, transparency, consent, and user-held data model). Such a uniform law would significantly curtail compliance costs and put the US on equal footing with other countries and regions (EU).

### **Solving cross-border data transfers with the user-held data model.**

The user-held data model could be incredibly impactful in solving cross-border data transfer problems.

### **Learning from the EU.**

In the past few years, the EU has adopted several regulations that aim to unlock data from silos and address some of the most complex issues concerning data use and AI. The US could consider learning from the EU and aligning the US regulatory landscape with the EU.

### **Further references:**

- **Paulius Jurcys, et al., 'The Future of International Data Transfers: Managing New Legal Risk with a 'User-Held' Data Model' *The Computer Law and Security Review* (2022, forthcoming), available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4010356](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4010356)**



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

**Focusing on User-Centric Solutions.** It is difficult to get privacy to work appropriately only by restricting the use of data by businesses and creating more regulations for technology. As emphasized above, data is also y valuable for individuals. The real long-term solutions should be based on models that empower individuals to manage and utilize their own data. In the past decades, companies have built successful businesses on data. As a result, five data giants dominate the digital space. However, solutions for individuals to make their life better and healthier based on personal data are still in a very early phase. This area offers many opportunities for innovations, economic growth, and improving the lives of individuals.

The best way to support this development is to offer individuals more rights and tools to access such user-generated data, create frameworks that help them own such data, and benefit from services and applications to utilize such user-held data.

### Possible actions for government agencies:

- Create incentives for direct-to-consumer sellers and service providers to adopt privacy labels explaining how they use their customer data;
- Promote user interface and user experience frameworks that are based on **opt-in** (rather than opt-out) approaches;
- Create **incentives** for data market participants to develop solutions that facilitate access to data. This could include API protocols, **open-source standards** for data portability, and data interoperability;
- Create programs to facilitate collaboration between academic organizations, think tanks, and market participants to conduct studies relying on **behavioral economics**. The end result could be to figure out areas where nudges could be useful to improve user experience, enhance transparency and nudge people to control better how their data is used;
- Consider areas where the government introduces **regulatory sandboxes** to validate the use of PETs.

**References:**

- **Paulius Jurcys et al., 'My Data, My Terms: A Proposal for Personal Data Use Licenses'**, *Harvard Journal of Law and Technology Digest* (2020), available at: <https://jolt.law.harvard.edu/digest/my-data-my-terms>

**7. Risks related to PETs adoption**

One of the dimensions of unintended consequences relates to rule-making: adopting rules in rapidly changing technological environments is challenging. The regulator needs to balance the necessary freedom for developing new privacy-enhancing technologies and complex compliance requirements that could restrict innovation. Imposing specific rules on the use of data could likely lead to the concentration of data in the hands of several organizations. The end result could be that individuals will not be able to get better services based on their own user-generated data.

**Further references:**

- **Mark Fenwick and Paulius Jurcys, 'From Cyborgs to Quantified Selves: Augmenting Privacy Rights with User-Centric Technology and Design'**, 13(1) JIPITEC (2022) available at: <https://www.jipitec.eu/issues/jipitec-13-1-2022/5512>

**8. Existing best practices that are helpful for PETs adoption**

Wearables can be a testament to the opportunity for more direct-to-individual applications. Some wearables companies (such as Ōura) could be an excellent example of how their products and applications could improve individual lives, personal health, and well-being through data. At Prifina, we aim to create an environment where anyone can build applications on top of user-held data and bring value closer to the user.

**Further references:**

- **Jouko Ahvenainen, 'People are interested in protecting personal data, although some deny it'** available at: [medium.com/prifina/people-are-interested-in-protecting-personal-data-although-some-deny-it-fc35977a712f](https://medium.com/prifina/people-are-interested-in-protecting-personal-data-although-some-deny-it-fc35977a712f)

- **Jouko Ahvenainen, 'Today's wearables are a bit like 1980s computers and that's not great'**, available at: [medium.com/prifina/todays-wearables-are-a-bit-like-1980s-computers-and-that-s-not-great-771afd58d2ca](https://medium.com/prifina/todays-wearables-are-a-bit-like-1980s-computers-and-that-s-not-great-771afd58d2ca)

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

In the current centralized/siloed data ecosystem, companies rely on product-centric business models; there is a lack of incentives to create user-centric services, i.e., services that offer value on a more individualized level. Currently, enterprises collect and generate the most value from personal data for their own corporate interests. Turning this around to benefit individuals more requires a collective change of mindset and incentives. It could be further incentivized through policy changes, making it easier for individuals to gather this data and shifting the reputational risk from building data monopolies for companies.

### Further references:

- **Jouko Ahvenainen, 'Who Protects Whom In The Battle For Personal Data And Privacy? You?'** available at: [medium.com/prifina/who-protects-whom-in-the-battle-for-personal-data-and-privacy-you-c267b5a48200](https://medium.com/prifina/who-protects-whom-in-the-battle-for-personal-data-and-privacy-you-c267b5a48200)
- **Jouko Ahvenainen, 'Turn it around — could businesses sell data to consumers?'** available at: [medium.com/prifina/turn-it-around-could-businesses-sell-data-to-consumers-705382cccc1](https://medium.com/prifina/turn-it-around-could-businesses-sell-data-to-consumers-705382cccc1)

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

The Prifina team has published a series of articles about the benefits of adopting the user-held model. Shorter articles are available at [www.medium.com/prifina](https://www.medium.com/prifina).