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

LeapYear Technologies

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 https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies

Responding party: LeapYear Technologies, Inc (https://leapyear.io)
Entity type: Industry / software provider
Respondent: Head of Marketing, Garrett Long

1. *Specific research opportunities to advance PETs:*
The federal government has a unique opportunity to provide the public with a consolidated summary of the current state of PETs usage / testing in the public sector today. In certain scenarios it's well publicized that a PET is used (for example Census), but there are many other situations where PETs may be in use or trial that are hard to find out (for example this DARPA program, it's hard to understand what happened and the result) By providing the public and legislators a "state of play" it would help determine the actual state of PETs usage, highlight success and failures, and potentially identify areas to focus on for advancement.

A potential useful framework to report on these federal projects would include:

- The agency(ies) involved
- A description of the privacy problem to be solved, including definition of threat models and attack vectors
- A review of the type of data involved
- The PET(s) used or considered
- Time of the project (start, duration)
- A summary of the result (success, failure, other)

A second opportunity would be for the federal government to assemble a canonical guide to what PETs are, the maturity of a given PET, what problems they are well suited for, and when a PET is not useful. This type of guide can be used to help agencies and the public streamline consideration and selection of PET(s). This type of guide can also include when multiple PETs may be useful in certain contexts.

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

The responses in this section will have to do with applications specifically for differential privacy.

In general, differential privacy solutions are well suited for applications that meet certain criteria:

- The data to be analyzed is sensitive (deemed so by regulation, law, contract or best practice)
- The data is structured / tabular
- The use case can tolerate a small and explainable amount of randomization in an analysis
- The analyst cannot (or should not) be trusted to receive access to row level data, but has legitimate purposes to query the data to reveal and use statistical properties contained therein

Sectors of application

Our work in the financial sector reveals many compelling use cases for differential privacy on market data. Market data can include consumer transactions (such as credit cards or bank accounts) and institutional data (such as equity transactions, fixed income pricing and over the counter traded derivatives). Generally, the financial sector is expected to, by regulation, provide appropriate liquidity, risk and best execution services for the market – ensuring a fair playing field for institutional and retail investors alike. Differential privacy has been proven in the private sector to have many useful applications under these considerations including:

- Helping asset managers receive best pricing from their banks
- Helping broker-dealers optimize demand forecasting (and by proxy) trading costs
- Helping protect citizens' financial behaviors while still enabling useful analysis of broader market trends
- Bringing new sources of information to derive investment strategies
- Eliminating unnecessary (and often mis-understood) leakage of private information

These same types of data analysis are routinely considered and executed by the financial regulatory bodies (including SEC and FINRA). Recent trends to require banks to hand over detailed transaction data sets (the consolidated audit tape) have created significant tension and public debate on how to secure this data and keep it private. Differential privacy software can be used to improve the public/private partnership in this area. Federal agencies with differentially private access to data sets can achieve many of the stated goals of oversight, without the need to stipulate massive data collection and storage which puts US institutions and citizens' privacy at risk.

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

HIPAA – today, HIPAA defines the mechanisms through which healthcare data can be modified (de-identified) and therefore deemed to protect the privacy of citizens whom are included in a data set. Unfortunately, the realities of information and computing power that is available today (due to the rise of digital systems) largely invalidates the assumptions under which the original regulation was written. Updating HIPAA (as has already been proposed) to require a more formal definition of privacy will help advance the adoption of PETs to protect the healthcare information of every US citizen.

SEC/FINRA – the SEC and FINRA enforce regulations on the financial services sector. Regulations are in place to ensure optimal market risk, liquidity and provide best execution to institutional and retail investors alike. These regulations often act in a way that reduces the sharing of data, either across an institution or with the larger ecosystem. Our work in the capital markets also reveals a mix of ad hoc methods, applied inconsistently across market participants, that attempt to deal with privacy issues. These methods often trap important signal in data sets, leading to assumptions that firms are safer than they really are and leaking privacy. The SEC and FINRA can motivate an industry standard on the way particular market data is protected and used leveraging PETs.

Treasury - The IRS collects sensitive demographic and income information on every citizen. The IRS also has the ability, and sometimes the requirement, to share and exchange this information with other federal, state, local and public agencies. But sharing this data or creating information products based on this data has inherent privacy risks. The IRS has already acknowledged the existence of shortcomings in the way they analyze data, and has explored using differential privacy to improve both data value and citizen privacy. Treasury can expand and formalize the use cases, risks and positive outcomes from the adoption of PETs for financial information. Regulations should be adopted in this particular set of use cases that would require the use of PETs to ensure citizens income and personal information is rigorously protected while still allowing the important and necessary work of the IRS and its partner agencies to continue.

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

As above, an update to HIPAA.