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

Bitfount

RFI Response: Privacy-Enhancing Technologies

Bitfount Ltd.

June 27, 2022

Bitfount Ltd. is a private company working to safely unlock the value of data for the benefit of humankind. Bitfount makes previously intractable data interactable. We do this through the development of a platform, based on the paradigm of federated data science, which removes barriers to data collaboration without compromising on data privacy or quality. As an interested party in OSTP's efforts to advance PETs, Bitfount is delighted to provide the following comments regarding OSTP's recent RFI.

Contact: Blaise Thomson, CEO;

Topic 1.

While there are a wide range of ongoing research activities in the PET field, most of those with which we've come into contact deal with the generation and development of the techniques themselves rather than how to develop standards such that they could be more easily adopted. The various players in the space will not be able to come to agreement on the development of standards for techniques which dictate what 'level' of privacy protection (in the form of epsilon for differential privacy, for example) or deployment requirements without a more overarching set of standards. We recommend investing both in the development of a set of standards around differential privacy, synthetic data, and secure multi-party computation with which all parties can live.

As an extension of this work, we recommend performing research into and developing easy on-ramps for businesses with PET-appropriate use cases. A large barrier to adoption is simply knowledge that PETs are an acceptable solution to data management and privacy challenges from the point of view of regulators. Research into how best to educate businesses and create incentives for adoption could go a long way.

Topic 2.

Current limitations of PETs include the sheer number of definitions of privacy, impact on accuracy of outputs, insufficient compute power, and lack of benchmarks in the field.

- **Definitions of privacy:** There are several definitions of privacy which have been developed overtime. We view this as a limitation of the PET field given the wide range of accepted definitions, even within a given PET technique, is likely to cause confusion among those who might adopt PETs. For a technology that is meant to reduce uncertainty, having so many complex options may lead to reluctance to adopt PETs by less-informed entities.

- **Impact on accuracy:** While PETs provide a useful mechanism for analyzing otherwise sensitive data, they do affect the accuracy of the output a data scientist receives from performing a query or running a model. This is a limitation of the technology in cases where algorithms are making decisions which could have real-life consequences for citizens. The accuracy loss can typically be quantified, but there is a tradeoff between accuracy and privacy leakage.

- **Insufficient compute power:** For the average organization, executing day-to-day business processes integrated with PETs would be too costly given they often require significantly more computational power than running data operations with no privacy-preserving techniques applied. Note, this includes time cost, as data science teams tend to prioritise speed and will not want to adopt a slower technology if it is not required.

- **Lack of benchmarks:** For techniques such as differential privacy, we as a collective industry do not have easily digestible benchmarks describing what level of privacy preservation is appropriate given the type of data you are using and the level of risk you can tolerate in association with the data. A lack of benchmarks for epsilon in various situations means we struggle to make it 'turnkey' for businesses to adopt PETs and understand what they need to implement.

Topic 3.

On a high-level, we believe techniques such as federated data science in combination with differential privacy can provide a viable solution to challenges such as enabling cross-border data transfer under a new version of Privacy Shield.

On a more tactical level, we see tremendous potential for the use of PETs in industries holding data typically considered sensitive or protected, but that could be 'unlocked' in the public interest if analysis were properly de-risked. These include healthcare and life sciences, defense, energy, and international trade and commerce.

- **Healthcare:** PETs can be leveraged in healthcare settings, especially during clinical trial design, execution, and post-trial analysis, to ensure HIPAA compliance while reducing data overhead. Additionally, we believe PETs have a place in enabling researchers to develop the next generation of digital biomarkers and diagnostic models without putting patient data at risk.

- **Defense:** PETs can be leveraged to improve data collaboration between allied countries, while minimizing risk to citizenry. PETs can add another layer of protection in data operations for government agencies or their contractors when performing machine learning or general data analysis. PETs can also

be leveraged to enforce data access and usage controls across various database systems within the defense sector.

- **Energy:** PETs can be leveraged to enable multi-party data consortia between energy companies and local authorities to monitor ESG goals without creating competitive risk.

- **International trade & commerce:** With PETs, we believe several multi-national companies would be able to better operate, while protecting the data sovereignty of a given nation's citizens. However, to unlock this use case, companies would need to better understand from regulators where the use of PETs to access data in a federated manner falls on the spectrum of x-border data transfer.

Topic 4.

We would value clearer guidance in relation to regulation or authorities on the following:

- A formal definition of anonymity with the use of PETs. At what point do regulatory bodies consider data activity to render individuals anonymous if PETs are in use?
- The introduction of federated data science as a mechanism to enable a version of Privacy Shield to protect x-border data transfer between the US and EU countries.

Topic 6.

There is concern in the field that the institutions investing most in the advancement, adoption, and development of PETs, namely Meta, Microsoft, Google, and IBM, are setting the agenda for how they will be used and in what contexts. We recommend developing an independent set of standards dictating when it is appropriate to leverage which kind of PETs and what thresholds are for different types of data, use cases, and levels of risk tolerance in a given enterprise. These would not be legal mandates, but rather would allow businesses to make informed decisions about how the data they've collected is leveraged as opposed to accepting the parameters laid out by these companies.