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

HUB Security Limited

HUB Security's response to the Office of Science and Technology Policy's Request for Information on Advancing Privacy-Enhancing Technologies

July 8, 2022

Organization	Hub Security Ltd
Organization type	Industry - Cyber Security
Respondent Person and Contact	Name: Gaurav Sharma Email: Role: VP, North America

Table of Contents

About HUB Security

HUB Security Limited ("HUB") was established in 2017 by veterans of the 8200 and 81 elite intelligence units of the Israeli Defense Forces. The company specializes in unique Cyber Security solutions protecting sensitive commercial and government information. The company debuted advanced confidential computing solutions aimed at preventing hostile intrusions at the hardware level while introducing a novel set of data theft prevention solutions.

HUB Security, a frontrunner in confidential computing hardware and software offerings, brings a fundamentally unique approach to prevent and mitigate the impact of present sophisticated cyber attacks by protecting the entire computing stack. With its military-grade ultra-secure hardware and software, HUB Security is capable of preventing cyber threats in any kind of environment while protecting critical assets such as data for all market segments. With HUB's technology, the compute platform is fully secured in one appliance or can turn any other computing environment into a secure compute platform.

Central to HUB's confidential computing solutions is its secured execution environment. The solutions are based on our hardware and software design used to protect any application and any data. We leverage a range of security mechanisms and a new security paradigm, HUB's confidential computing, aiming to isolate any application and associated elements within its own secure execution environment. This includes the application, data, AI models, policies for access or approval, audit trails and logs, and all cryptographic keys, services and key management.

HUB operates in over 30 countries and provides innovative cybersecurity computing appliances as well as a wide range of cybersecurity services worldwide.

2. *Specific technical aspects or limitations of PETs*

The multiple existing approaches to PET constitute a patchwork of narrow solutions to the specific problems in the privacy domain of data and applications. Each technique creates a basic tradeoff between the capability to achieve the application goals and the level of privacy protection. Several leading examples are:

1. Homomorphic encryption techniques enable complete privacy in theory by enabling encrypted applications to work on the encrypted data sets. The main penalty is extreme computational load, which makes large scale use in the cloud and in real time impractical and prohibitively expensive. Moreover, the data and the application code must be prepared in advance to be compatible with the technique, thus creating cumbersome and specific processes as a barrier to automation and simplicity of use.
2. Another option is to keep the sensitive data at the location of its origin and bring the applications to the data location, as in federated learning technique for AI models. The AI model trains on the subsets of the entire dataset and is enhanced by exchanging the training anonymized metadata coefficients. In this case the data privacy is preserved relative to the cloud provider, but the AI model accuracy and quality are reduced, since it is not trained on the entire combined data set from all sources.
3. The third option is putting the data into proprietary hardware secure enclaves such as Intel SGX, AMD SEV, which are basically just RAM partition inline encryption by the CPU. All the data and application code in the encrypted space of the CPU memory can be accessed only from the inside of this space. CPU proprietary hardware enforces access control to the allocated memory address space. This approach is growing today in popularity at the public clouds (Microsoft Azure, Google) as the solution to the Confidential Computing challenge. This is a very attractive option as the CPU is already present in the servers. It protects against local malicious access attempts to the specific memory regions - and that's it. It does not handle the Admin insider threat or remote access to the encrypted partition via correct credentials. Furthermore, the proprietary non-public implementation by the manufacturer prevents community review for the protection and exhibits its own vulnerabilities (as has been found multiple times in the mentioned implementations). The end user does not control the encryption keys and does not know the quality of the random numbers used to generate these keys inside the CPU silicon. In any privacy technique controlling the obfuscation key is the basic means of controlling the privacy of the data.

Looking forward, the truly useful PET should not impact the original goals of working with private and sensitive data, by enabling full computational throughput on multiple types of CPUs and providing multi layered protection centered on the data and working against multiple threat types

simultaneously. The main principle of it is isolation between data and data consumers, data sources, data users, infrastructure, etc. The isolation on the finest available level enables an implementation of zero trust architecture and continuous enforcement of the proper access to the data.

Additionally, any PET tool must be easily upgradable, as technology is always advancing and the attackers get access to better tools. For example, the rapid development of quantum computing created a huge gap and clear danger of exposing past, current and future state/enterprise level secrets and all the world communications in the 10 to 30 years from now. The upgrade from classical cryptographic algorithms to post quantum cryptography is looking like a long complicated and expensive process, because the infrastructure was not built to be upgradable. The basic assumption should be that every PET will be broken eventually and so must support easy and quick updates to its core functionality to prevent breach of privacy.

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

The following are the areas that will benefit and have high potential for adoption of PETs:

- **Multi-Party Analytics**: Analytics and in particular AI usage will be used everywhere to automate and handle the exponentially increasing amount of data. It is a fundamental truism of artificial intelligence that the more data it is fed, the better it performs. This technology can, for example, help hospitals to more efficiently allocate beds, staff, medicine, and accessories. It can provide practitioners with life-saving speed by delivering data & insights at the moment they need it. Similarly, such technologies can facilitate fraud analysis across financial institutions to fight cybercrime.

  However, most data is siloed among different health systems, financial institutions, departments, etc to conform to regulations and meet internal security policies. The ability to safely collaborate on AI projects without compromising privacy & security and meeting regulatory requirements is a major challenge. For example, sharing medical images and AI models across multiple medical institutions or fraud analysis across financial institutions, requires a high level of security, privacy and processing power.

  Confidential computing can provide the ability to create isolated environments to protect the integrity and privacy of models and data and can be used to safely unlock the data for multi-party analytics.

- **Edge Computing**:
  Edge computing holds massive potential to transform lives with new innovations and lead to massive economic growth. To give you an idea, IDC is projecting that worldwide spending on edge computing will reach $250 billion by 2024. Massive amount of data will be generated and consumed at the edge - a stat from Gartner says that data generated at the edge will increase from 10% today to 75% by 2025. This data and the resulting intelligence will become the competitive advantage for enterprises.

  With the dramatic increase in broadband due to the Infrastructure Investment and Jobs Act and the desire to reduce long haul bandwidth needs, real time and low latency services will collect and process a dramatic amount of data locally. These services will become a major value add revenue generator. But these are often places where privacy has been challenging yet increasingly critical such as regional healthcare, mobile communications, public safety infrastructure, transportation, financial systems, etc.

- **Industry 4.0**: The Fourth Industrial Revolution (4IR) is an amalgamation of advanced capabilities mixing artificial intelligence (AI), robotics, the Internet of Things (IoT), Digital Twins, quantum computing, genetic engineering, and other technologies. 4IR is driving major transformation in the Industrial sector with smart autonomous systems fueled by data and machine learning. Connected things with tremendous volumes of data have created smart factories and systems that can perform predictive maintenance, remote monitoring and optimize production without human intervention. IoT & Digital Twins have made simulations and maintenance extremely efficient. This area is a natural securing, this is a natural extension of edge computing and AI as discussed above. The massive amount of data and insights are natural starting points for PETs.

All 16 critical infrastructure sectors (as defined by Cybersecurity and Infrastructure Security Agency (CISA)) will be impacted by the above technological advancements and will benefit the most from adoption of PETs.

7. Risks related to PETs adoption

The following are the risks and challenges related to PETs adoption:

Data Utility: Since data serves as the key ingredient that will drive economies and improve lives using innovations mentioned previously, PETs should be implemented to make sure that the data does not get stripped of its expected utility. While implementing privacy and security controls to an individual's data is extremely important, it also needs to be able to be used to its maximum extent to serve the individual and the larger population directly. For example, age or gender might be an important attribute of a person that needs to be treated confidentially, but completely removing it while diagnosing the person for a medical condition can have a catastrophic impact.

Redundant Encodings: On the flip side, PETs can give a false sense of security that good controls have been implemented to preserve privacy but other attributes called redundant encodings can be used to deduce the attribute that has been protected. For example, given the location, condition and race of a person seeking medical treatment, her age can be deduced. A more comprehensive approach is needed to identify all relevant attributes if PETs that protect data privacy by obscurity are adopted and in many cases these approaches might not be feasible to be implemented correctly.

Explainability: When algorithms are used to make decisions, explaining the path used to make the decision can be extremely difficult if the attribute has been protected. For example, why a load application was denied might be difficult to explain if the data was protected. Some PETs that use a black box approach for analytics or decision making, will pose a challenge both from technical and regulation perspectives. Sectors such as healthcare and financial services, will be heavily impacted by this limitation.

Expertise: Given the complex nature of many PETs, specific skills are needed and at the current moment the talent pool is extremely limited. There are many innovators but large scale adoption needs a concerted effort to promote these approaches and attract the right talent.

Quantum Threat: Many approaches to PETs use complex encryption algorithms but are susceptible to quantum computing based attacks. PETs should consider post quantum readiness to address imminent threats posed by other nation states and adversaries.

In addition to the above, there are many unknown unknowns that can introduce complexity and gaps that require a larger public-private collaboration.

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

Data is the new resource that will introduce many new economic opportunities and transform our lives. Technologies such as Artificial Intelligence, edge computing and others will leverage rich amounts of data to unleash new innovations. These innovations will improve our healthcare, offer equitable access to services, improve our safety and help us address some of the existential threats such as climate change.

However, the same data and technologies can be used to knowingly monitor, deny access, subjugate, oppress or incarcerate individuals or entire sections of a population by an authoritarian regime or unknowingly discriminate, misinform or lead to identity theft by a large corporation. Regulations like CCPA and GDPR have laid the groundwork but there are still too many loopholes that have to be addressed.

PETs have come a long way and there are many approaches that can be used individually or in combination to protect data privacy while facilitating data sharing for the innovations mentioned above. However, PETs need to be combined with the other best practices for data security for increasing their efficacy. One proposed approach is to combine data privacy with security and resiliency efforts led by CISA.

Another key threat is related to quantum computing. President Biden signed a National Security Memorandum in May 2022, outlining the Administration’s plan to address the risks posed by quantum computers to America’s cybersecurity. However, most PETs currently do not factor the impact of quantum computing to data privacy and there needs to be a concerted effort to factor that threat in.

Effective PETs need to be adopted quickly. Data will unleash many new capabilities that will improve our lives but without effective PETs, the same data can hold us hostage knowingly or unknowingly.