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

Accenture

July 9, 2022

Dr. Alondra Nelson
Acting Director
Office Science and Technology Policy
Re: Advancing Privacy-Enhancing Technologies (Docket Number: 2022-12432)

Dear Director Nelson,

As a leading global professional services company, Accenture provides a broad range of services and solutions in strategy and consulting, technology, interactive, and operations, that span all industries. We combine artificial intelligence (AI) with deep industry and analytics expertise to help our clients embrace these emerging, intelligent technologies confidently and responsibly and our 710,000 employees serve clients in more than 120 countries.

We are committed to create lasting change at the intersection of technology and human ingenuity for our business and communities. Our clients reach virtually every American consumer and rely on data and digital platforms to deliver products and services. Businesses that treat data collection and data strategy as part of the consumer experience will benefit from greater consumer willingness to share information.

We are committed to partnering with our clients to protect consumer privacy and support the establishment of a national consumer privacy law to protect consumers, promote innovation and advance U.S. competitiveness. Additionally, Accenture Labs, which began conducting R&D on Privacy Enhancing Technology in 2015, are developing a new framework for privacy-preserving data cooperatives. With a well-designed cooperative, companies can share data and collaborate without concerns around trust, compliance, privacy and data control or ownership. There are many technological techniques available to make this possible; confidential computing, homomorphic encryption and multiparty computation can all contribute. Another, often overlooked, benefit of privacy enhancing techniques is their potential for alleviating reliance on those energy-intensive technologies.

We appreciate the opportunity to submit comments to the Office of Science and Technology Policy ‘s Request for Information on “Advancing Privacy-Enhancing Technologies” and look forward to continuing to support your efforts.

Sincerely,

Paul Daugherty
Group Chief Executive – Technology & Chief Technology Officer
Accenture

Accenture
Comments to Office of Science and Technology Policy
Advancing Privacy-Enhancing Technologies
July 9, 2022

Question 1: ***Specific research opportunities to advance Privacy Enhancing Technologies (PETs):***

While PETs are certainly beneficial in improving collaboration between entities and mitigating data privacy concerns, they are currently slow, expensive, and come at a large computational cost. Accenture strongly supports increased funding for research and development of classical PETs including privacy assessments and protection mechanisms for Differential Privacy, Federated Split Learning (FSL), Homomorphic Encryptions and Secure-Multi-Party Compute (MPC) solutions including cloud-based versions of such solutions to reduce computational costs, decrease risks of data breaches, and speed up data processing. In addition, Accenture supports the Department of Energy's (DoE) current research of a Quantum Internet, which could be accelerated to explore specific quantum-information protection techniques.

Questions 2 & 9: ***Specific technical aspects or limitations of PETs: Existing barriers to PETs adoption:***

<u>Homomorphic Encryption</u>

The main limitation to mainstream adoption of Homomorphic Encryption is the computational intensity and cost of the processing. These factors limit the amount of data that can practically be used, which currently makes the process extremely slow, rendering it impractical and expensive for real-time or near real-time processing. Additionally, because the data remains encrypted throughout the process and there may be limits on the types or number of operations that can be performed, it is essential for the data processor and data owner to have agreements in place around the structure and content of the data as well as the processing that will take place so that the data processor cannot interrogate or experiment with the data.

<u>Secure Multi-Party Communication</u>

The main drawback to utilizing Secure Multi-Party Communication (MPC) technologies are the high computational costs needed to operate. MPC's require a lot of communication between parties, which can add further latencies during the computation process. Another factor with some MPC's is the complexity of representing a business problem as a logical circuit with a compliant structure, which can require some specialist skills. From a security perspective, one point to note is that MPC's don't protect against "poisoning" attacks, where one of the parties could attempt to maliciously influence the results of queries by another party by intentionally

using false or misleading data to intentionally lead to an answer which is not correct (i.e., exaggerating or understating a statistical result to drive another party to draw incorrect conclusions).

Quantum Information Based Privacy & Security Techniques

As we advance to a Quantum-Internet, meeting DiVincenzo's criteria for Quantum computing and communications, Quantum-Information security and privacy preservation techniques will be needed. Additionally, quantum security and privacy techniques could provide an alternative to classical PETs, which in their current versions are slow, vulnerable, and costly to operate.

Accenture has been ideating in quantum data privacy and security techniques. One of those techniques, US Patent Application #20220014364 - QUANTUM INFORMATION INTERCEPTION PREVENTION offers the strongest privacy, confidentiality and security currently conceivable. This invention promises to preserve security and privacy even against adversaries with unlimited resources, time and perfect knowledge (e.g., knowing protocols and cipher secrets). Technical aspects of this invention involve entangling a user's information qubit with two or more ancillary qubits and gate-cipher(s)—which together function as a quantum-key the user can control. The owner of this quantum-key would have the ability to control when, how and if the original information inside the protected qubit would be communicated or shared with another.

Additionally, this invention would enable the determination of whether the original information in the qubit was modified and provide the option to destroy the quantum-keys, thus effectively disabling the information in the protected qubit by making it incoherent. This information disablement happens even if the protected information qubit is no longer in control of the owner. This remote disablement aspect would be desirable if the information qubit is stolen or if the owner no longer consents to disclosing private information.

This invention also has the ability for private multi-party quantum computation. A quantum computer can perform non-measurement-based operations on the protected information qubit without access to the quantum-keys and return it to the owner. The owner can maintain physical control of the quantum-keys, guaranteeing that even if the other party attempted to decrypt or measure the qubit, they would only receive a random result which does not reveal any of the private information. If an adversary gained unauthorized access or control of a protected qubit and its quantum-keys, the adversary would only have one chance to reverse the quantum gate-ciphers on the entangled ancillary qubits.

We encourage the investment in quantum-based techniques as Quantum will enable a new paradigm of privacy and security techniques enabled by quantum computers and the quantum internet.

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

Industry is increasingly leveraging data to improve analysis and decision-making—creating more personalized experiences for customers and greater operational efficiency. Currently, due to PET's limited capacity, the use cases of homomorphic encryption for multi-party ML are limited and only used in the inference phase. However, Federated Learning (FL) and Federated Split Learning (FSL) are better solutions for multi-party learning in the training phase. Initiatives and investments should include FL and FSL. Differential Privacy, Data Sanitization and Data Anonymization are also very impactful techniques that should be factored in to achieve or enhance privacy. As technology continues to improve, there is a wide variety of sectors that would benefit from PET's.

Healthcare:

The healthcare industry has some of the strictest regulations for data privacy and security. Homomorphic encryption could allow the healthcare industry to leverage machine learning services for crucial insights into areas such as medical diagnostics, leading to faster, more accurate diagnoses and more effective treatments.

A relevant healthcare use case to look to would be the MyHealthMyData (MHMD) program. MHMD, an EU-funded project, is looking at how to share anonymized data for medical care, research and development, while giving people ownership over their health data. The platform combines blockchain, smart contracts, dynamic consent and a comprehensive suite of data privacy and secure analytics tools including Homomorphic Encryption and MPC.

Financial Services:

Financial organizations are also under strict regulations for maintaining privacy of customer information. In decisions, such as loan or credit approvals that involve data from multiple owners/sources, Homomorphic Encryption can keep financial information secure while still allowing for the automation of predictive tasks such as loan approval and know your customer (KYC) services using machine learning.

Service Checks:

PETs will also be valuable in the aviation, railway, manufacturing, oil and gas industries, where we're seeing techniques like federated learning and SMPC utilized to predict the condition of in-service equipment or identify the root cause of an equipment failure. In these industries, an equipment vendor needs to collect data from many different customers and environments simultaneously to monitor and predict parts deterioration and optimal maintenance times. These vendors operate independently and by practice do not share performance data. Multi-party ML training, enabled by FL and SMPC, allows a model to both train and have inferences across these privately held datasets.

Another, often overlooked, benefit of privacy enhancing techniques is their potential for alleviating reliance on those energy-intensive technologies. Linking our long term privacy goals with our long term sustainability goals may bring additional attention, prioritization, and investment.