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

R3

R3 Response to the Office of Science and Technology Policy Request for Information on Advancing Privacy-Enhancing Technologies

July 2022

R3 welcomes the opportunity to respond to the Office of Science and Technology Policy's (OSTP) Request for Information (RFI) on advancing privacy-enhancing technologies (PETs).

We are encouraged by OSTP's launch of the interagency Fast Track Action Committee within the National Science and Technology Council to develop a vision and national strategy for privacy-preserving data sharing and analytics.

We support OSTP's stated goal of "putting forth a vision for responsibly harnessing privacy-preserving data sharing and analytics to benefit individuals and society." We also agree with a recent OSTP blog post titled, "Advancing a Vision for Privacy-Enhancing Technologies," in which the authors conclude "we believe PETs can help enable progress in these key areas, from improving healthcare and combatting financial crime, to responding to natural disasters and driving next-generation digital technologies with equity in mind and in a manner that upholds our democratic values."[1]

Government and institutions have the power to effect positive, transformational change by exploiting and combining the data they hold. Such information can be used to help policymakers address important social issues such as social and health inequalities, human trafficking, and climate change. However, many of these benefits have not been realized due to the equally important need to preserve the privacy of individual citizens. PETs represent an opportunity to realize the myriad of benefits on offer from wider data sharing while simultaneously guaranteeing the rights and privacy of individuals.

It is for this reason R3 believes that the future of computing is confidential and that PETs, particularly confidential computing mechanisms built on Trusted Execution Environments (TEEs), are key to enabling this future. To that end, we stand ready to engage with U.S. policymakers as they work constructively on this critical topic and to assist in the development of a national strategy on privacy-preserving data sharing and analytics. We are keen to serve as a resource for OSTP and the Fast Track Action Committee as they consider actions to bolster responsible and effective PET adoption in the United States.

Below we outline our approach to many of the PET-related issues raised in this RFI. We would be delighted to discuss our response in more detail at any time.

Introducing R3

R3 is a New York-based enterprise software company that enables direct, digital collaboration in regulated industries where trust is critical. Multi-party solutions developed on our platforms, Corda and Conclave, harness the "Power of 3" – R3's trust technology, connected networks, and regulated markets expertise – to drive market innovation and improve processes in banking, capital markets, global trade, insurance, and other sectors.

As the only company to deliver both a private, secure, and scalable distributed ledger technology (DLT) platform designed for regulated markets, and a confidential computing platform, R3 empowers

[1] OSTP's blog post on PETs can be accessed here: https://www.whitehouse.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/

institutions to realize the full potential of trusted direct collaboration in the new digital economy. We maintain one of the largest DLT production ecosystems in the world, connecting over 400 institutions in both the private and public sectors.

Introducing R3's Trust Technologies: Conclave and Corda

Corda is R3's DLT software, which is used throughout regulated financial industries to record, manage and execute institutions' financial transactions in perfect synchrony with their peers. Corda is unique in the blockchain space by offering an open core model alongside privacy, settlement finality, and scalability.

Developed in collaboration with our ecosystem, Corda is transforming entire industries by digitalizing the processes and systems that firms rely on to connect and transact with each other. The Corda ecosystem is the largest in the world with more than 400 institutions deploying and building on Corda Enterprise and Corda. Our customers and partners have access to a network of leading systems integrators, cloud providers, technology firms, software vendors, corporates, and banks.

Building on the success of Corda, and in reaction to the increasing digitization of personal data, we developed Conclave, a software development kit and suite of complementary cloud services for the rapid development of privacy-first applications using hardware TEEs.

Conclave Core utilizes confidential computing and Intel Software Guard Extensions (SGX) technologies to empower businesses to develop applications that can analyze sensitive data from multiple parties – all without compromising on confidentiality. It also allows firms to securely aggregate their datasets to solve shared business problems for their customers across markets and, crucially, without revealing the actual data to anyone.

A wide variety of institutions can be transformed by building on Conclave, including financial services firms, analytics firms, companies leveraging artificial intelligence (AI) and machine learning (ML), data service providers, exchanges, fraud detection and compliance software firms, corporates, and regulators.

Conclave offers a range of benefits for customers, including access to previously inaccessible client data to discover new insights, and the ability to:

- Deliver collaborative data services to grow and differentiate their businesses;
- Monetize data-driven insights without sacrificing an individual's privacy or an institution's processes;
- Reduce the risk of third-party misuse of customer data;
- Simplify building of a privacy-preserving application to collect and process confidential data from customers;
- Benefit from cutting-edge technologies such as confidential computing to secure data at the hardware level; and
- Provide high-value analytics to customers by building apps on a platform that assures multi-party data privacy.

R3's Confidential Computing Observations

The rise and proliferation of the Internet into all facets of life, a process which began in the 2000s and has rapidly accelerated during the COVID-19 pandemic and ensuing pivot to hybrid work, has delivered many benefits but also significant data privacy risks.

Businesses are facing new challenges in this changing world in which more confidential data is being stored and shared online than ever before. Many organizations seek to address potential risks by simply not sharing confidential data with their ecosystem partners in order to prevent tampering or leaks. This results in unintended economic costs and prevents organizations from realizing the benefits of data-driven insights.

Confidential computing, a type of PET that is built on hardware TEEs and encrypts data while it is still in the processing stage, can enable organizations to securely aggregate their datasets to solve shared problems for customers across markets, without revealing raw confidential and personal data to anyone.

A recent report by the Everest Group forecast the confidential computing Total Accessible Market (TAM) to grow to $54 billion by 2026, a striking total that illustrates the sheer scope and importance of this emerging technology.[2] U.S. policymakers should work with industry and other stakeholders to foster innovation as well as consumer protection and trust in these new technologies.

Working with OSTP

R3 believes that the work of OSTP is essential to fostering responsible and robust adoption of PETs. We have long recognized the value of working with policymakers and regulators to support their efforts relating to emerging technologies and look forward to further assisting as this important work progresses.

If you have any questions relating to our submission, please contact:

Michael Greco, Government Relations Policy Manager:
Isabelle Corbett, Global Head of Government Relations:

Responses to Selected Questions

Below are R3's responses to selected questions that are most relevant to our perspective as a technology provider.

1. ***Specific research opportunities to advance PETs:*** **Information about Federal research opportunities that could be introduced or modified to accelerate the development or adoption of PETs. This includes topics for research, hardware and software development, and educational and training programs. This also includes information about specific techniques and approaches that could be among the most promising technologies in this space.**

As OSTP explores the broad topic of PETs and formulates a national strategy, we encourage it to include hardware TEEs. We believe that TEEs are certainly among the most promising technologies in this space for a variety of reasons and can accelerate the development and adoption of PETs.

TEEs are a hardware-based solution that allow programs to operate inside secure enclaves which are isolated from the rest of the computer on which they run. They also ensure that data and code can be processed without the computer's owner gaining access to the raw data. As a result, programs are resistant to physical and software attacks by the owner or operator of a computer, as well as by outside

[2] Everest Groups' paper, "Confidential Computing – the Next Frontier in Data Security," can be accessed here: https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/10/Everest_Group_-_Confidential_Computing_-_The_Next_Frontier_in_Data_Security_-_2021-10-19.pdf

parties. In this example, organizations that share data with partners by utilizing TEEs can be assured that the raw data will not be shared and cannot be tampered with.

In our experience, TEEs are an effective, efficient, and flexible confidential computing technique, while being both highly scalable and production ready. TEEs also can run all code inside its secure enclave – an improvement from many other PETs which limit the number of use cases that can be addressed.

Additionally, R3 urges the U.S. government to bolster its research and development activities to support fundamental research on PETs, with a focus on the relationship between PETs and AI and ML technologies. Specifically, we encourage OSTP to coordinate and spearhead research initiatives exploring how both AI and ML can be leveraged in combination with TEEs. TEEs do have the capability to leverage data-driven technologies like AI and ML while preserving data privacy, but more research and development would benefit the overall adoption of PETs.

We also recommend that the National Artificial Intelligence Initiative, which is administered by OSTP, consider TEEs when evaluating PET's interplay with AI and ML technologies. ML models in particular benefit from large, diverse training data sets, and their emergence as a mainstream technology has revealed the importance of multiple firms being able to share data securely. For ML models to function effectively, it often requires trust in a data aggregator. In sensitive applications, such as healthcare and financial services, the potential leak of trade secrets and risk of privacy breaches can prevent data sharing.

2. ***Specific technical aspects or limitations of PETs:*** **Information about technical specifics of PETs that have implications for their development or adoption. This includes information about specific PET techniques that are promising, recent or anticipated advances in the theory and practice of PETs, constraints posed by limited data and computational resources, limitations posed by current approaches to de-identification and deanonymization techniques, limitations or tradeoffs posed when considering PETs as well as technical approaches to equity considerations such as fairness-aware machine learning, security considerations based on relevant advances in cryptography or computing architecture, and new or emerging privacy-enhancing techniques. This also includes technical specifications that could improve the benefits or privacy protections, or reduce the risks or costs of adopting PETs.**

[No response]

3. ***Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs:*** **Information about sectors, applications, or types of analysis that have high potential for the adoption of PETs. This includes sectors and applications where data are exceptionally decentralized or sensitive, where PETs could unlock insights or services of significant value to the public, where PETs can reduce the risk of unintentional disclosures, where PETs might assist in data portability and interoperability, and sectors and applications where the adoption of PETs might exacerbate risks, including in the areas of privacy, cybersecurity, accuracy of data analysis, equity for underserved communities, and economic competition. This topic covers opportunities to improve the effectiveness of data sharing among specific Federal agencies and between specific Federal agencies and entities outside the Federal Government, including the goals outlined in Section 5 of Executive Order 14058: Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government.**

Confidential computing is broadly applicable across a wide range of sectors and industries but will likely offer the most significant near-term benefits to sectors and applications where data are extremely sensitive, such as the financial services, healthcare, and public sectors. Each of these sectors process large quantities of personally identifiable information (PII) and other sensitive data.

As an example of confidential computing's benefits for a sector where the processed data are extremely sensitive, consider the Hope for Justice charity, a nonprofit that collects data on human trafficking. The data gathered by Hope for Justice is based on highly sensitive, individual cases that often contain PII. Before the advent of confidential computing, analysis of the charity's data may very well have been impossible because any leaks in the original data could threaten the precarious position of those who provide it. One solution has been to apply blockchain along with confidential computing, allowing the charity to create aggregated analytics about human trafficking trends without exposing the underlying data and people's personal information. In one country, these technologies pinpointed a 35-mile radius from which 95 percent all domestic human trafficking reports originated. This information provided the relevant authorities the intelligence they needed to locate and stop the traffickers.[3]

Additionally, we note that a range of data collaboration use cases can be unlocked with this technology. For example, R3's Conclave enables collaboration with its focus on developer and user experience, as well as its support of many coding languages which unlocks large developer communities. Users of Conclave can use high-level coding languages such as Java, Kotlin, Python, and JavaScript to develop hardware-secured services and privacy-first applications.

We also note that R3's Conclave offers both code integrity and data integrity. Importantly, this functionality enables us to deliver technical proof through remote attestation reports in which code is executed without being altered.

R3's Conclave can open several business use cases for software vendors to process previously inaccessible data and build high-value analytics solutions. With cutting-edge PET, the Conclave platform allows businesses to capitalize on Market Data Aggregation, Fraud Detection, Private Order Matching, and Analytics Solutions. We explore these four challenge areas in greater detail below:

- **Challenge 1: Market Data Aggregation:** Firms need to know how big their market is in order to calculate their own market share and forecasts; however, they do not feel comfortable sharing proprietary sales data such as new and recurring license revenue with a third-party provider.
    - **Solution:** Conclave enables firms to securely upload revenue and other proprietary sales data to a service that calculates relevant statistics, all without allowing the operator of the system to see the raw data, saving time and costly development resources.

- **Challenge 2: Fraud Detection:** Fraud that is spread across multiple institutions often remains undetected as there has been no way to securely pool multiple private data sets from industry participants to identify and prevent fraud. This challenge impacts both the private and public sectors. There are limits to the types of services that fraud detection software vendors can provide as there are data privacy regulations and concerns with sharing confidential customer data with a third party.

[3] "Blockchain is restructuring ESG." Alisa DiCaprio, Chis Ford, Yingying Zhang. https://www.r3.com/blog/blockchain-is-restructuring-esg/

- **Solution:** Conclave enables fraud detection software firms to access these private data sets by providing assurances to their customers that their data will not be viewed by the provider or the provider's other customers, just processed. As a result, these software firms can build new solutions that aggregate data from multiple firms in a trustworthy manner, while reducing false positives and detecting new fraud. In the public sector, federal departments and agencies that distribute benefits to the public could utilize this technology to detect fraud and error by comparing other government data sets without needing to examine individual records that could contain confidential data.

- **Challenge 3: Private Order Matching:** Traders often want to do price discovery and order matching privately, and want to make sure that no one – not even the market operators – can misuse their private transaction details.
  - **Solution:** Conclave enables firms to build private order matching solutions that give assurances that private transaction data will not be viewed or misused. As a result, software firms can build solutions that protect market participants' data, giving traders and regulators confidence that they are trading in a fair and transparent marketplace.

- **Challenge 4: Analytics Solutions:** Companies want to benefit from insights that Analytics and AI firms can provide, but do not feel comfortable sending confidential data outside of their organization, or having it pooled with their peers.
  - **Solution:** Conclave enables Analytics and AI firms to deliver solutions that provide transparency into how data is processed and assurances that customer data is protected. This enables end users to benefit from insights derived from analytics solutions without having to compromise on data privacy. Software firms can either build new solutions or develop on existing analytics solutions and run them across new private data sets.[4]

4. *Specific regulations or authorities that could be used, modified, or introduced to advance PETs:* Information about Federal regulations or authorities that could be used, modified, or introduced to accelerate the development or adoption of PETs. This includes privacy-related rulemaking authorities under the Office of Management and Budget, the Federal Trade Commission, and financial regulatory bodies, as well as acquisition regulations under the Federal Acquisition Regulations. This also includes the Federal authority to set procedures for agencies to ensure the responsible sharing of data. This also covers hiring authorities to recruit Federal employees with expertise to advance PETs, as well as acquisition authorities (e.g., Other Transaction Authority) to procure PETs for development.

We encourage the U.S. government's hiring authorities to recruit federal employees with the necessary expertise to advance effective PET technical standards. A robust federal workforce with strong technical skills and knowledge would benefit the entire PET sector. It is important for federal agencies and departments to develop in-house expertise that enables robust and advanced PET projects and initiatives that bolster innovation while applying the necessary controls to protect consumers. Recently, the Office of Personnel Management (OPM) outlined a detailed skills-based hiring guide for federal agencies, which could serve as a template for recruitment of federal employees with PET expertise.[5]

[4] More information on R3's Conclave and the problems it can solve can be accessed here: https://www.r3.com/wp-content/uploads/2020/10/Conclave_Platform_FS_R3_2020.pdf

[5] OPM's Skills-Based Hiring Guidance can be accessed here: https://www.opm.gov/news/releases/2022/05/release-opm-releases-skills-based-hiring-guidance/

R3 also encourages the Office of Management and Budget, Federal Trade Commission (FTC), and other federal agencies that issue privacy-related rulemakings to consider benefits offered by confidential computing as they explore and issue regulations and other guidance to ensure the responsible sharing of data.

Overall, the PET sector would benefit from the development of voluntary consensus standards and best practices that provide useful and actionable guidance. In certain cases, clear regulations that effectively balance consumer protection while promoting innovation and adoption may be necessary and ultimately useful. Improving consumer protection and fostering innovation are complementary goals – increased consumer protection can bolster public trust which in turn will lead to increased adoption of PETs.

5. *Specific laws that could be used, modified, or introduced to advance PETs:* Information about provisions in U.S. Federal law, including implementing regulations, that could be used, modified, or introduced to accelerate the development or adoption of PETs. This includes provisions, safe harbors, and definitions of use, disclosure, safeguards, and breaches. Information may also include comments on how to advance PETs as part of new or proposed legislation, such as that which would create a National Secure Data Service. Information may also include comments on State law or on international law as it applies to data sharing among international entities.

As of July 2022, five U.S. states (California, Colorado, Virginia, Utah, and Connecticut) have passed their own respective comprehensive consumer data privacy laws. This growing patchwork of state-level privacy laws complicates compliance for businesses and may ultimately harm consumer protection efforts. U.S. consumers and businesses utilizing PETs would both benefit from clear and comprehensive regulation.

We also encourage OSTP to continue to promote cross-agency collaboration with NIST, the National Science Foundation, the Federal Trade Commission, and other relevant federal agencies and departments. A harmonized whole-of-government approach to PETs would benefit both the sector and consumers. We also encourage the U.S. government to continue its collaboration and cooperation with foreign governments, including the United Kingdom, on prize challenges and related initiatives to foster PET adoption.

6. *Specific mechanisms, not covered above, that could be used, modified, or introduced to advance PETs:* This includes the development of open-source protocols and technical guidance, the use of public-private partnerships, prize challenges, grants, testbeds, standards, collaborations with foreign countries and nongovernmental entities, the Federal Data Strategy, and data sharing procedures with State, local, tribal, and territorial governments. This also includes interpretations and modifications of standard non-disclosure agreements, confidentiality clauses, data use or sharing agreements, etc.

R3 believes that all the mechanisms referenced in the above question (open-source protocols and technical guidance, the use of public-private partnerships, prize challenges, grants, testbeds, standards, collaborations with foreign countries and nongovernmental entities, the Federal Data Strategy, and data sharing procedures with State, local, tribal, and territorial governments) have the potential to advance PETs.

Open-source software is particularly important because it accelerates trust in the technology and removes barriers to adoption via a variety of features including internal audits.

Additionally, we believe there is a clear need for increased public awareness and understanding of PETs. The U.S. government can help promote greater awareness of PETs, including confidential computing, and the opportunities they present through prize challenges and collaborations. We also believe that technical standards, if developed in a collaborative and inclusive process, can benefit the PET industry. NIST has a particularly strong record of developing voluntary, consensus-based standards that promote innovation while applying the necessary controls to encourage consumer protection.

We appreciate and support the U.S. and UK joint Prize Challenges to Accelerate Development and Adoption of Privacy-Enhancing Technologies. We support the prize challenges' feature of enabling innovators to engage with regulators, including the UK's Financial Conduct Authority and the U.S. Financial Crimes Enforcement Network. Collaboration between industry and regulators, along with increased public awareness, are key measures to maximizing the potential of these technologies, and we appreciate the U.S. and UK governments' willingness to address both factors.

Finally, as U.S. policymakers evaluate federal standards that can be used, modified, or introduced to address PETs, we encourage NIST to update its Privacy Framework and Cybersecurity Framework to keep pace with recent PET developments.

7. *Risks related to PETs adoption:* Identification of risks or negative consequences resulting from PETs adoption as well as policy, governance, and technical measures that could mitigate those risks. This includes risks related to equity for underserved or marginalized groups, the complexity of implementation and resources required for adoption, as well as from conceptual misunderstandings of the technical guarantees provided by PETs. This also includes recommendations on how to measure risk of PETs adoption and conduct risk-benefit analyses of use.

[No response.]

8. *Existing best practices that are helpful for PETs adoption:* Information about U.S. policies that are currently helping facilitate adoption as well as best practices that facilitate responsible adoption. This includes existing policies that support adoption, including in the areas of privacy, cybersecurity, accuracy of data analysis, equity for underserved communities, and economic competition. This also includes information about where and when PETs can be situated within tiered access frameworks for accessing restricted data, ranging from publicly accessible to fully restricted data.

We encourage the U.S. government to collaborate with industry and other stakeholders to develop a shared taxonomy and terminology of PETs, following a public comment period. A common, well-designed taxonomy could cultivate trust in the design, development, use, and governance of PETs while raising public awareness and providing greater clarity. NIST's Taxonomy and Terminology of Adversarial Machine Learning[6] is a useful template that U.S. institutions could look to when considering this taxonomy.

Additionally, we believe the U.S. government should work with a broad and inclusive range of stakeholders to develop guidance and, in certain cases, clear rules governing how regulated entities use PETs. The PET industry would benefit from clear rules of the road that govern PET usage for specific data classifications, particularly when PII or other confidential data are shared.

[6] NIST's Taxonomy and Terminology of Adversarial Machine Learning can be accessed here: https://csrc.nist.gov/publications/detail/nistir/8269/draft

9. *Existing barriers, not covered above, to PETs adoption:* Information about technical, sociotechnical, usability, and socioeconomic barriers that have inhibited wider adoption of PETs, such as a lack of public trust. This includes recommendations on how such barriers could be overcome. Responses that focus on increasing equity for underserved or marginalized groups are especially welcome.

As discussed in our response to Q8, a shared taxonomy that clearly defines relevant terms would foster wider adoption of PETs. Such a taxonomy could provide the clarity needed to accelerate PET market growth.

Additionally, as also discussed in our response to Q8, the U.S. government can help promote prize challenges and other educational initiatives to increase public trust in and adoption of PETs. We encourage OSTP and the broader U.S. government to evaluate ways to build trust among underserved and disadvantaged Americans in an equitable and inclusive way.

10. *Other information that is relevant to the adoption of PETs:* Information that is relevant to the adoption of PETs that does not fit into any of the topics enumerated above.

We encourage OSTP to refer to our confidential computing white paper, "Conclave: An Introduction," written by R3's Chief Technology Officer, Richard Gendal Brown.[7]

[7] R3's Conclave white paper can be accessed here: https://www.conclave.net/wp-content/uploads/2022/01/ConclaveIntroductoryWhitepaper.pdf