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

Fortanix Inc.

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.

From:
To: PETS-RFI
Subject: < RFI Response: Privacy-Enhancing Technologies >
Date: Friday, July 8, 2022 2:59:06 PM
Attachments:

Response of Fortanix, Inc. to the OSTP RFI "Notice of request for information on Advancing Privacy-Enhancing Technologies".

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.

   Confidential Computing, defined as "the protection of data in use using Trusted execution Environments"[1] (TEEs), is an emerging PET that is forecast to experience exponential market growth to 2026.[2]
   Confidential Computing has been successfully applied by Fortanix to a variety of use-cases where enforcement of data privacy and application security is necessary including: cryptographic key management (e.g. the Fortanix Data Security Manager™ product, with FIPS 140-2 Level 1 software certification[3] and FIPS 140-2 Level 3 hardware certification[4]), federated machine learning (FML), multi-party data analytics, private information retrieval, confidential artificial intelligence (AI) – model training and inference, and confidential blockchains. These use-cases are applicable to a range of industry requirements, encompassing healthcare, financial services, retail, supply chain management, decentralized applications (Web 3.0), and U.S. Federal Government agencies.

   The announced bilateral innovation prize challenges focused on privacy-enhancing-technologies (PETs)[5] could include specific challenges associated with the development or implementation of Confidential Computing.

   Since publication of the National Privacy Research Strategy in 2016[6], Confidential Computing has become available at scale through integration within general purpose computing platforms provided by public cloud service providers and OEM hardware vendors. Initiation of a technical comparison of different PETs and their appropriate application by the NSTC and/or NIST would encourage evaluation by potential end-users. Such an evaluation would also provide contemporary information to lawmakers and a basis for communication of public information on how Confidential Computing can protect private data while innovation through the secure integration of discrete datasets for in-depth analysis.
   Confidential Computing represents one of the most promising PETs under development today, due to its flexibility of deployment, functional scope, and suitability for multi-party analytics and artificial intelligence applications. In the latter case, the ability for a regulatory agency to interrogate and verify the deployed software code is important for the "explainability" and transparency of models. Alternative, cryptography-based, PETs to Confidential Computing obfuscate software code, preventing analysis of system functionality.

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.

   Confidential Computing incorporates attestation of Trusted Execution Environments (TEEs). Attestation provides auditable cryptographic validation of the integrity of a TEE and the software code deployed inside it. Mutual attestation of applications and enforced verification of attestation credentials creates segmentation of processes and supports robust software supply chain security.

   Extension of Confidential Computing beyond CPUs to include GPUs will provide broad capability for secure machine learning and deployment of artificial intelligence, including deep learning with massive neural networks.

   Confidential Computing represents one of the most promising PETs under development today, due to its flexibility of deployment, functional scope, and suitability for multi-party analytics and artificial intelligence applications. In the latter case, the ability for a regulatory agency to interrogate and verify the deployed software code is important for the "explainability" and transparency of models. Alternative, cryptography-based, PETs to Confidential Computing obfuscate software code, preventing analysis of system functionality.

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 can provide sufficient data and applications security to enable recommendation of the technology by Federal Government, in accordance with the provisions of Exec. Order No. 14,034 (2021)[7]. Where data privacy is required to protect national security, the use of Trusted Execution Environments (TEEs), with process-based identity verification and software integrity validation through attestation, is consistent with the concept of Zero-Trust Architecture, mandated under Executive Order No. 14,028 (2021)[8].

   Fortanix has demonstrate the application of Confidential Computing to support clinical AI validation in healthcare[9], directed towards rare disease diagnosis and therapeutic design, and genome analysis using foreign data sources that are subject to different privacy legislation (e.g., EU GDPR). These use-cases highlight the benefits of Confidential Computing for healthcare, including applications within the internet-of-medical-things (IoMT) and telemedicine.

   As part of an investigation related to the secure acquisition of real-world data (RWD) by the FDA, Fortanix demonstrated how Confidential Computing enables data portability through end-to-end encryption of private healthcare data (PHI) sourced from different healthcare providers, within a distributed network.[10] The reference architecture developed could be transferred to meet the needs of other U.S. Government agencies and could incorporate individual-level interaction via secure IoMT devices or controlled access to electronic health records (eHR) – as has been demonstrated in Germany, using Fortanix Confidential Computing technology within a national framework for patient privacy.[11]

   Confidential Computing has also been successfully demonstrated for financial crime detection, including anti-money laundering[12] and synthetic identity fraud[13]. As decentralized finance (DeFi) solutions proliferate, it will be increasingly important for national and international regulatory agencies to support analysis of private financial data, hosted by independent financial institutions. Confidential Computing provides an effective method of facilitating scalable, transnational, data analysis without any requirement for sensitive data to be shared between collaborating parties. This capability of Confidential Computing offers law enforcement agencies the ability to detect financial crime, without any need to access the underlying data or compromise data sovereignty requirements of partner states.

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.

   Organizations that have identified privacy and security benefits in the adoption of Confidential Computing are often slow to implement this form of PET due to perceived risks to compliance with Federal regulations. Fortanix has successfully demonstrated the capability of Confidential Computing to secure protected data and sensitive software code for customers in financial services, healthcare, and US Government Agencies. Industry customers, however, typically remain constrained in their adoption of PETs and their plans to deploy data and applications using untrusted cloud infrastructure, by concerns that PETs do not address legislative requirements with respect to protected data and applications. Such protected data may include PII and PHI that is subject to security and privacy controls under the provisions of the Fair Credit Reporting Act (FCRA) [15 U.S.C §1681: §602(a)(4)][14], the Gramm-Leach-Bliley Act [15 U.S.C. §6801(V)(A): §501(a), and 15 U.S.C. §6821(V)(B): [15]

§521], and/or The Health Insurance Portability and Accountability Act of 1996 (HIPAA) [12 U.S.C. 1811(II)(F): §264(c)(1)][16].

Explicit reference to Confidential Computing and other PETs within existing and future legislation that incorporates, or amends, data privacy requirements would clarify the terms of compliance with respect to privacy obligations for industry. An example of one opportunity to encourage adoption of Confidential Computing would be recognition of the additional security provided by Trusted Execution Environments (TEEs) within the Federal Information Processing Standards (FIPS) defined by NIST. This is particularly relevant to the secure management and enforced privacy of cryptographic keys that underpin identity management within today's internet and that will be the foundation of tomorrow's, predicted, Web 3.0 decentralization.[17]

The revision of existing legislation to clarify approved methods of data privacy protection, to include a list of potential cyberattack vectors to be mitigated by technical solutions, would be assist organizations in evaluating their compliance with specific industry requirements. Such clarifications would also support audit and enforcement of data privacy and definitions of "best practice" by Federal regulators and law enforcement agencies.

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.

Organizations that have identified privacy and security benefits in the adoption of Confidential Computing are often slow to implement this form of PET due to perceived risks to compliance with Federal regulations. Fortanix has successfully demonstrated the capability of Confidential Computing to secure protected data and sensitive software code for customers in financial services, healthcare, and US Government Agencies. Industry customers, however, typically remain constrained in their adoption of PETs and their plans to deploy data and applications using untrusted cloud infrastructure, by concerns that PETs do not address legislative requirements with respect to protected data and applications. Such protected data may include PII and PHI that is subject to security and privacy controls under the provisions of the Fair Credit Reporting Act (FCRA) [15 U.S.C §1681: §602(a)(4)][18], the Gramm-Leach-Bliley Act [15 U.S.C. §6801(V)(A): §501(a), and 15 U.S.C. §6821(V)(B): §521][19], and/or The Health Insurance Portability and Accountability Act of 1996 (HIPAA) [12 U.S.C. 1811(II)(F): §264(c)(1)][20].

Explicit reference to Confidential Computing and other PETs within existing and future legislation that incorporates, or amends, data privacy requirements would clarify the terms of compliance with respect to privacy obligations for industry.

The revision of existing legislation to clarify approved methods of data privacy protection, to include a list of potential cyberattack vectors to be mitigated by technical solutions, would be assist organizations in evaluating their compliance with specific industry requirements. Such clarifications would also support audit and enforcement of data privacy and definitions of "best practice" by Federal regulators and law enforcement agencies.

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.

Recent publication of NIST IR 8320[21] provides helpful guidance on the requirement for, and implementation of, Confidential Computing technology within cloud and edge-based deployments. However, it has been incumbent upon industry to elucidate practical applications of PETs to address real-word privacy and security needs. It would be helpful if NIST and agencies responsible for data privacy enforcement collaborated with leading technology and service providers to establish reference architectures that are applicable to compliance with specific legislation. Such architectures could be vendor agnostic or, in common with NIST IR 8320, a survey of applicable technologies and services could be provided to direct PET adopters to appropriate partners for implementation.

The development of reference architectures incorporating PETs might also drive technical convergence and standardization within industry to reduce barriers to implementation created by price differentiation and poor interoperability. In the case of Confidential Computing, there is active work within industry to address problems created by heterogenous approaches to Trusted Execution Environment (TEE) attestation – this work is being led by the Confidential Computing Consortium of the Linux Foundation[22] and the Remote ATestation procedureS (RATS) working group of the Internet Engineering Task Force (IETF)[23], however, there is no national, nor international, policy reference to align these industrial initiatives. Establishing reference standards for PET deployment in support of data privacy protection, including open-source protocols for attestation and identity assertion, would provide a framework within which industry could direct future technical research and work with authorities to improve legislation and enhance technical standards.

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.

Implementation of PETs typically requires a sophisticated set of skills, including advanced software engineering, cryptography, and software solution architecture. In the case of PETs such as Fully Homomorphic Encryption (FHE), Multi-Party Computing (MPC), and Confidential Computing, the knowledge required to undertake and evaluate system design and implementation can prove a barrier to adoption. Increasing provision of packages service models, such as the Fortanix Confidential AI managed service[24], allow non-technical users (e.g., data analysts and end-users) to take advantage of privacy-preserving computation by providing hosted infrastructure and auditability of deployment, to demonstrate compliance with privacy regulations.

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.

Executive Order No. 14,028 (2021)[25] and the publication of NIST Special Publication 800-207 "Zero-Trust Architecture"[26] (ZTA) has generated increased interest in Confidential Computing as a PET that supports identity authentication, software isolation, and network resilience. Confidential Computing can be used as a generic PET solution to encapsulate end-to-end workflows, such is in a federated machine learning (FML) architecture, or it can be implemented to secure specific data processing operations. Fortanix has demonstrated the application of a private-information retrieval (PIR) solution for U.S. Government agencies that supports secure search of public data and integration of unclassified data with restricted data for private query by data analysts. This solution protects the identity of the analyst, the content of the classified data query, and demonstrates performance advantages (i.e., reduced system latency) compared to alternative cryptography-based PETs.

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.

Implementation of PETs typically requires a sophisticated set of skills, including advanced software engineering, cryptography, and software solution architecture. In the case of PETs such as Fully Homomorphic Encryption (FHE), Multi-Party Computing (MPC), and Confidential Computing, the knowledge required to undertake and evaluate system design and implementation can prove a barrier to adoption. Increasing provision of packages service models, such as the Fortanix Confidential AI managed service[27], allow non-technical users (e.g., data analysts and end-users) to take advantage of privacy-preserving computation by providing hosted infrastructure and auditability of deployment, to demonstrate compliance with privacy regulations.

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.

The “CIA triad” of confidentiality, integrity, and availability is fully supported by Confidential Computing as a form of PET: Confidentiality of private data is maintained through encryption of related memory in use. Software integrity can be asserted using “measurement” of deployed application code as part of the intrinsic attestation process that underpins deployment of robust Trusted Execution Environments (TEEs). Availability is supported by Confidential Computing due to the isolation guarantees that enable approved software to be safely executed, even where the underlying hardware or network infrastructure has been compromised by a cyber threat actor.

Recent research has elucidated the extended loiter time of cyberattackers within networks before detection and mitigation of the intrusion.[28] Confidential Computing provides a means to ensure data privacy where processing occurs on untrusted infrastructure – which should be assumed under a Zero-Trust Architecture (ZTA) approach to system design. Where computation takes place using distributed resources over which the application owner has no control, Confidential Computing can provide systemic resilience by supporting continued, secure, data processing until network reconfiguration is complete.

In response to identified threats to national security disclosed by CISA[29] and the FBI[30], alongside international partners, Confidential Computing can be employed as a PET to secure the data privacy of U.S. citizens, to protect the confidentiality of intellectual property, and to prevent unchecked network exploitation through attestation-based identity verification and isolation of software from privileged system users. These capabilities are of particular importance within the context of cyber-physical systems, where the risk to critical infrastructure and the potential for physical harm to U.S. citizens is acute.[31]

[1] Available from: https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/03/confidentialcomputing_outreach_whitepaper-8-5x11-1.pdf [Accessed: July 8, 2022].

[2] Available from: https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/10/Everest_Group_-_Confidential_Computing_-_The_Next_Frontier_in_Data_Security_-_2021-10-19.pdf [Accessed: July 8, 2022].

[3] Available from: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3326 [Accessed: July 8, 2022].

[4] Available from: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3545 [Accessed: July 8, 2022].

[5] Available from: https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/ [Accessed: July 8, 2022].

[6] Available from: https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf [Accessed: July 8, 2022].

[7] Available from: https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries [Accessed: July 8, 2022].

[8] Available from: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity [Accessed: July 8, 2022].

[9] Available from: https://www.beekeeperai.com/blog/58111-securing-healthcare-ai-with-confidential [Accessed: July 8, 2022].

[10] Available from: https://www.intel.com/content/www/us/en/newsroom/news/leidos-fortanix-accelerate-clinical-trials.html#gs.583ork [Accessed: July 8, 2022].

[11] Available from: https://www.gesundheitsindustrie-bw.de/en/article/news/ehr-and-phr-digital-records-in-the-german-healthcare-system [Accessed: July 8, 2022].

[12] Available from: https://www.fortanix.com/company/pr/2022/04/intel-fiverity-and-fortanix-bring-confidential-computing-to-the-fight-against-digital-fraud-in-financial-services [Accessed: July 8, 2022].

[13] Available from: https://www.fortanix.com/company/pr/2022/04/intel-fiverity-and-fortanix-bring-confidential-computing-to-the-fight-against-digital-fraud-in-financial-services [Accessed: July 8, 2022].

[14] Available from: https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf [Accessed: July 8, 2022].

[15] Available from: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf [Accessed: July 8, 2022].

[16] Available from: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf [Accessed: July 8, 2022].

[17] Available from: https://www.darkreading.com/endpoint/me-my-digital-self-and-i-why-identity-is-the-foundation-of-a-decentralized-future [Accessed: July 8, 2022].

[18] Available from: https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf [Accessed: July 8, 2022].

[19] Available from: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf [Accessed: July 8, 2022].

[20] Available from: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf [Accessed: July 8, 2022].

[21] Available from: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320.pdf [Accessed: July 8, 2022].

[22] Available from: https://confidentialcomputing.io/webinar-the-future-of-attestation-in-a-confidential-world/ [Accessed: July 8, 2022].

[23] Available from:
https://datatracker.ietf.org/wg/rats/about/#:~:text=Remote%20attestation%20procedures%20(RATS)%20determine,links%20to%20the%20supply%20chain.
[Accessed: July 8, 2022].

[24] Available from: https://www.fortanix.com/products/confidential-ai [Accessed: July 8, 2022].

[25] Available from: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity [Accessed: July 8, 2022].

[26] Available from: https://csrc.nist.gov/publications/detail/sp/800-207/final [Accessed: July 8, 2022].

[27] Available from: https://www.fortanix.com/products/confidential-ai [Accessed: July 8, 2022].

[28] Available from: https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/ [Accessed: July 8, 2022].

[29] Available from: https://www.cisa.gov/uscert/ncas/current-activity/2021/07/19/us-government-releases-indictment-and-several-advisories-detailing
[Accessed: July 8, 2022].

[30] Available from: https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi [Accessed: July 8, 2022].

[31] Available from: https://www.darkreading.com/physical-security/outlining-risks-to-the-world-s-vital-cyber-physical-systems [Accessed: July 8, 2022].

Dr Richard Searle
Vice President of Confidential Computing
Fortanix®, 800 West El Camino Real, Suite 180, Mountain View, CA 94040, USA
Fortanix' mission is to solve cloud security and privacy.