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

BurstIQ

RFI: Request for Information on Advancing Privacy-Enhancing Technologies

Response by:

Frank Ricotta, Chief Executive Officer
Wendy Charles, PhD, Chief Scientific Officer
Robert Lubeck, Chief Growth Officer

BurstIQ, Inc.
9635 Maroon Circle, #310
Englewood, CO 80112

QUESTIONS:

1. Specific research opportunities to advance PETs:

Response:

We believe that the current generation of PET is fast approaching its event horizon. Some technical advances may extend the horizon based on the current approach that requires further research and new methods that will change the fundamental paradigm.

Specific topics include:

Privacy Enhanced Data: There exists a fundamental flaw in the underlying premise of PET solutions. Many proposals focus on systems and not on the data. These systems erroneously assume that data does not inherently contain any intelligence. Therefore, organizations take a traditional systems approach to data protection by controlling access to the data, where/how data may be processed, and/or techniques that protect sensitive information through anonymization. However, we believe that a significant untapped area for further research should focus on a data-centric approach with Privacy-Enhanced Data (PED). At BurstIQ, we describe this as “smart data” or “trusted data.” The foundation of PED is based on the concept that data can become “self-aware data objects.” In short, PED is a new data construct that fuses context

and trust attributes with the data itself into a new data object instead of managing these attributes in the surrounding systems. With data attributes such as metadata, rights, source, origin, chain of custody, time, place, and use permissions, PEDs can then provide key parameters to PET solutions to drive their behavior. Several methods can maintain the integrity of a PED and verify key attributes. Specifically, blockchain methodology offers a solid foundation for signing/attesting PEDs and tracking ownership, use, and authentication. Please review our Smart Data White Paper at https://burstiq.com/smart-data-white-paper/ or by requesting the PDF from info@burstiq.com to learn more about PED capabilities.

Generative Adversarial Networks (GANs): GANs are a form of artificial intelligence (AI) where at least one AI network focuses on learning while at least one other AI network focuses on judging the behavior of the first. While not necessarily designed for privacy protections per se, GANs support how data is used–or not misused–in intelligent systems.

Extended trust to the edge: We believe there is a lot of promise around W3C digital identity frameworks with trust anchors, W3C Verifiable Credentials, and non-fungible tokens (NFTs) related to individual privacy and data ownership.

Scalability: Additional research is needed to improve the scalability of many PETs. For example, while zero-knowledge proofs and homomorphic encryption have the potential to extend the current approach event horizon, the technologies are currently too slow and immature to gain wide-scale adoption (Sharma et al., 2020; Tomaz et al., 2020).

2. Specific technical aspects or limitations of PETs:

Response:

We advise against overly optimistic utilization of any technology as a panacea for privacy-related issues. Instead, advocate for a layered privacy approach in the manner organizations should approach cybersecurity.

Concerning de-identification, synthetic data transformation offers an excellent alternative to identifiable data for hypothesis generation or feasibility analyses; however, synthetic data is not typically sufficiently accurate to generate diagnostic/treatment algorithms (Raghunathan, 2021).

Further, tokenizing attribution fields offer another potential option. While this approach can maintain statistical significance, current techniques require the creation of duplicate data sets.

Last, these methods' next evolution should be real-time based on a trusted presentation driven by access, ownership, and permissions, which requires PED as a foundational capability.

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

Response:

PETs are particularly beneficial for providing individuals' health-related data for the healthcare and life sciences industries and protecting intellectual property in any industry.

Elaborating on the *health-related research industry*, researchers frequently obtain de-identified health information from electronic health record systems, data repositories, or data marketplaces. However, de-identified data create challenges for data linking and (by nature of being de-identified using the HIPAA Safe Harbor provision in 45 CFR § 164.514(b)(2)) lack dates of service necessary for assessing longitudinal trends for an individual or population. For these circumstances, we recommend tokenizing attribution fields.

Federate learning is also promising PET for any collaboration involving the need to share data or algorithms among collaborators without revealing intellectual property. As an example of these solutions, the MELLODDY Project is a collaboration of 10 pharmaceutical companies that share algorithms to improve the predictive capacity of molecular compounds for drug discovery (Burki, 2019). The partnership uses the Owkin blockchain to maintain molecular compounds in each pharmaceutical company's own servers and refine the algorithms using each's private data without sharing proprietary molecular compounds with each other. Only the algorithm is shared using a blockchain-based federated learning protocol.

4. Specific regulations or authorities that could be used, modified, or introduced to advance PETs:

Response:

First, we'd like to caution legislators that privacy-preserving technologies alone are not sufficient to protect individuals' sensitive information. Specifically, the concept of de-identification has become largely an illusion, with consideration that data scraping and matching require little more than basic programming and analytics skills to link data sets (Chiauzzi & Wicks, 2019; Narayan & Felten, 2014). While PETs can reduce exposure to individually-identifiable information, we advocate for modifications of the current federal HIPAA Privacy Rule to include more comprehensive privacy protections than the outdated list of HIPAA identifiers at 45 CFR § 164.514(b)(2)(i) to factor capabilities of data linking with modern computing.

Next, as a health information technology provider, we request more protections for the privacy of 365,000 health-related apps not subject to the HIPAA Privacy and Security Rules (Help Net Security, 2021). We applaud the progress of the American College of Physicians and the American Telemedicine Association in creating the *Digital Health Assessment Framework (2022)* and the Federal Trade Commission's (FTC) *Mobile Health App Best Practices (2016)*.

While these are valuable guidelines, there is no requirement for software developers to use these guidelines, resulting in significant vulnerabilities to the privacy of health information for an estimated 23 million U.S. users (Help Net Security, 2021). Unfortunately, there are few consequences for breaches, and there has been no FTC enforcement of the 2009 Health Breach Notification Rule to date (FTC, 2021). We urge the Federal Trade Commission to implement and enforce more stringent privacy protections for health information not subject to HIPAA regulations.

5. Specific laws that could be used, modified, or introduced to advance PETs:

Response:

First, we would like to use this section to dispel the falsehood that blockchain-based privacy-preserving strategies (as a blanket statement) are incompatible with the General Data Protection Regulation (GDPR) or U.S. privacy requirements. Blockchain compatibility with laws or statutes that mandate the "right to be forgotten" or the "right to be deleted" depends entirely on the platform and programming utilized. Several published methods provide direction for programming methods for actual data or obfuscation that meet the letter and spirit of these regulations (e.g., Herian, 2020; Yang et al., 2020). Further, a European Commission report–written in part by one of us (WC) through the European Observatory Blockchain Observatory and Forum–determined that health-oriented blockchains can meet GDPR requirements if designed appropriately (Livitckaia et al., 2022). For an extensive overview of blockchain compliance with U.S. regulations for health-oriented research, please read a journal article authored by one of us (Charles et al., 2019, https://doi.org/10.3389/fbloc.2019.00018).

Second, there is a growing patchwork of privacy statutes in U.S. states (Lively, 2022). While there is considerable overlap in the nature of privacy protections, the unique nature of some states' privacy requirements involves extensive software customization to meet these unique requirements. We advocate for a federal privacy act, similar to GDPR, that unifies the state-level statutes to allow for more straightforward programming and consistent approaches to designing PETs.

6. Specific mechanisms not covered above that could be used, modified, or introduced to advance PETs:

Response:

We advocate for creating PET technology-specific standards that would allow organizations to design and implement PETs responsibly and with more confidence. The National Institutes of Standards and Technology has created a Privacy-Enhancing Cryptography Project (2017) and published an excellent overview of cryptography-based PET (Brandão & Peralta, 2021) as a

starting point. We encourage the development of specific standards that software developers could utilize for best practices.

With gradual advances made in quantum computing–that will render some passwords and hashing algorithms obsolete in 5-10 years (Fedorov et al., 2018), we also advocate for standards that will reduce the likelihood that quantum computing could defeat some of the current PET approaches.

Finally, we would like to see significant advancements in digital identity standards to include technical constructs extending to data "ownership" and revocation methods. Also, we advocate for regulatory frameworks that clearly state that individuals have the right to "own" and manage their digital identities and data–especially their health data.

7. Risks related to PETs adoption:

Response:

We view centralized governance as the primary risk for PETs. Specifically, data privacy remains at risk when organizations insist on owning and controlling individuals' data with minimal oversight or transparency.

With the emergence of Web3 technologies built on distributed governance, there is a risk that regulatory agencies not infringe on this market innovation and inadvertently encourage centralized data control. For more information on trusted governance structures, please review the section on governance at https://burstiq.com/trust-as-a-differentiator-protecting-human-data-in-your-products-and-services-burstiq/.

Government agencies have a role in creating frameworks for proper data rights and appropriate uses. For example, when individuals are presented with options for conducting business with an organization or using a website, we advocate for "opt-in" data permissions instead of the typical default of "opt-out."

8. Existing best practices that are helpful for PETs adoption:

Response:

We advocate for thorough risk assessments and staff training, regardless of the technologies used for managing sensitive information. Organizations are also encouraged to perform ethical risk assessments (e.g., Allen et al., 2020; LaPointe & Fishbane, 2019) to identify vulnerabilities in particular populations, including the prospect that certain age groups, individuals who lack

access to broadband technology or sufficient computing devices, or individuals with physical or cognitive disabilities may lack access to PETs.

9. Existing barriers, not covered above, to PETs adoption:

Response:

There must be a clear delineation between uses of PETs and uses of private data. We recognize that government agencies cannot oversee all data utilization. However, agencies should provide standards and frameworks that drive interoperability, shift data ownership from Big Tech to individuals, and improve cybercrime enforcement.

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

We advocate for a clear and consistent definition of "privacy-enhancing technology," and what types of technology would be included in a solution framework.

Further, data rights and ownership should be foundational to the entire suite of PET solutions. Presently, there is a near-complete lack of clarity on this topic.

Last, AI should also be a key focus going forward with frameworks about AI ethics, bias, and digital twin civil rights as an extension of a person.

REFERENCES:

Allen, M., Vasiliu-Feltes, I., Ingraham, A., Mysore, I., Vaughn, M., & Charles, W. (2020). *Blockchain ethical design framework for healthcare*. Government Blockchain Association. https://www.gbaglobal.org/blockchain-ethical-design-framework-for-healthcare/

Brandão, L. T. A., & Peralta, R. (2021, November 3). *Privacy-enhancing cryptography to complement differential privacy*. https://www.nist.gov/publications/privacy-enhancing-cryptography-complement-differential-privacy

Burki, T. (2019). Pharma blockchains AI for drug development. *The Lancet*, *393*(10189), 2382. https://doi.org/10.1016/S0140-6736(19)31401-1

Charles, W., Marler, N., Long, L., & Manion, S. (2019). Blockchain Compliance by Design: Regulatory Considerations for Blockchain in Clinical Research. In *Frontiers in Blockchain* (Vol. 2). https://doi.org/10.3389/fbloc.2019.00018

Chiauzzi, E., & Wicks, P. (2019). Digital trespass: Ethical and terms-of-use violations by researchers accessing data from an online patient community. *Journal of Medical Internet Research*, *21*(2), e11985. https://doi.org/10.2196/11985

Digital Health Assessment Framework, V1. (2022, June 24). https://confluence.external-share.com/content/94649754-10cd-4803-9b67-91c784673d70

Federal Trade Commission. (2016, April 4). *Mobile health app developers: FTC best practices*. http://www.ftc.gov/business-guidance/resources/mobile-health-app-developers-ftc-best-practices

Federal Trade Commission. (2021, September 15). *Statement of the Commission on breaches by health apps and other connected devices*. https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

Fedorov, A. K., Kiktenko, E. O., & Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. *Nature*, *563*(7732), 465–467. https://doi.org/10.1038/d41586-018-07449-z

Help Net Security. (2021, February 12). *mHealth apps consistently expose PII and PHI through APIs*. https://www.helpnetsecurity.com/2021/02/12/mhealth-apps-expose-pii-phi-through-apis/

Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, *12*(1), 156–174. https://doi.org/10.1080/17579961.2020.1727094

LaPointe, C., & Fishbane, L. (2019). *The blockchain ethical design framework*. Georgetown University. https://beeckcenter.georgetown.edu/wp-content/uploads/2018/06/The-Blockchain-Ethical-Design-Framework.pdf

Lively, T. K. (2022, June 9). *US state privacy legislation tracker*. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Livitckaia, K., Charles, W., Larrañaga Piedra, U., Niemerg, M., Hasselgren, A., & Papadopoulou, E. (2022). *Blockchain applications in the healthcare sector*. European Union Blockchain Observatory & Forum: An initiative of the European Commission. https://www.eublockchainforum.eu/sites/default/files/reports/eubof_healthcare_2022_FINAL_pdf.pdf

Narayan, A., & Felten, E. W. (2014). *No silver bullet: De-identification still doesn't work*. Princeton University. https://www.cs.princeton.edu/~arvindn/publications/no-silver-bullet-de-identification.pdf

National Institute of Standards and Technology | Computer Security Resource Center. (2017, January 3). *Privacy-enhancing cryptography*. CSRC | NIST. https://csrc.nist.gov/projects/pec

Raghunathan, T. E. (2021). Synthetic data. *Annual Review of Statistics and Its Application*, *8*(1), 129–140. https://doi.org/10.1146/annurev-statistics-040720-031848

Sharma, B., Halder, R., & Singh, J. (2020, January). Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption. *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*. 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India. https://doi.org/10.1109/comsnets48256.2020.9027413

Tomaz, A. E. B., Nascimento, J. C. D., Hafid, A. S., & De Souza, J. N. (2020). Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 204441–204458. https://doi.org/10.1109/access.2020.3036811

Yang, J., Onik, M. M. H., & Kim, C.-S. (2020). Blockchain technology for protecting personal information privacy. In M. Ahmed (Ed.), *Blockchain in data analytics* (pp. 122–144). Cambridge Scholars Publisher. https://books.google.com/books/about/Blockchain_in_Data_Analytics.html?id=z_zLDwAAQBAJ