From: Sunny Kang <sunny@inpher.io>
Sent: Thursday, October 24, 2019 4:45 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments by Inpher

Dear Ms. Katie MacFarland,

Please find attached Inpher's comments on the preliminary draft of the NIST Privacy Framework (Federal Register Notice: https://www.federalregister.gov/documents/2019/09/09/2019-19315/preliminary-draft-of-the-nist-privacy-framework). Thank you very much, and we appreciate the opportunity to submit our comments.

Sincerely,

Sunny Seon Kang

Sr. Privacy Counsel, Head of Policy

(510) 289-4985

⊕ inpher, inc.

October 24, 2019

National Institute of Standards and Technology
U.S. Department of Commerce

100 Bureau Drive
Gaithersburg, MD 20899
ATTN: Katie MacFarland

Re: Preliminary Draft of the NIST Privacy Framework

Inpher appreciates the opportunity to advise the National Institute of Standards and Technology ("NIST") on the Preliminary Draft of the *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*.[1] NIST guidelines play an authoritative role in standardizing technical definitions and best practices across industries, and in educating regulators on the impact of emerging technologies. We support the emphasis of the NIST Privacy Framework in optimizing beneficial uses of data while minimizing adverse consequences for individual and societal privacy.

It is indeed timely to reject the outdated assumption that deriving value from data requires a privacy tradeoff. Standard-setting bodies and regulators should support the development of innovative approaches to protecting individuals' privacy and increasing trust in products and services. Fortunately, advances in privacy-enhancing technologies ("PETs") offer systemic, operational, and technical safeguards to data that simultaneously fulfill legal and regulatory obligations. Inpher submits the following comments to elucidate the application of cryptographic privacy safeguards to the data ecosystem, and the public value of standardizing PETs in privacy risk management.

Inpher Background

We are a US-based cryptography and machine-learning company with the conviction that encryption and privacy are foundational to the future of computing and commerce. Inpher applies years of academic research on Fully Homomorphic Encryption ("FHE") and secure Multi-Party Computation ("MPC") into commercially-ready applications that financial institutions are using in production today.[2]

Inpher's customers include some of the world's largest multinational financial institutions that use our software platform for privacy-preserving analytics and computation with mathematical guarantees of data security and sovereignty. This 'secret computing' technology enables compliant data processing across siloed departments, cross-jurisdictional and cross-industry information sharing, and zero-knowledge cloud computing, as the host never 'sees' the data nor has access to the keys. Our legal

[1] Federal Register, A Notice by the National Institute of Standards and Technology, *Preliminary Draft of the NIST Privacy Framework* (Sept. 9, 2019), https://www.federalregister.gov/documents/2019/09/09/2019-19315/preliminary-draft-of-the-nist-privacy-framework

[2] Inpher, *Case Studies*, https://www.inpher.io/case-studies-1#case-studies

and public policy department facilitates public education on privacy-preserving technologies and advocates for data protection by design, global privacy, and algorithmic accountability.

Overview of Cryptographic Privacy Safeguards

Cryptographic technologies can provide a solution to traditional tradeoffs in privacy and analytical precision (for example, with differential privacy methods), and allow secure collaboration across data silos for greater coordination and scalability. Advances in MPC and FHE allow functions to be performed on encrypted data without revealing the underlying information. Therefore, cryptographic PETs such as MPC and FHE offer incorruptible *ex ante* privacy safeguards against unauthorized access by intermediaries and third parties.[3]

Organizational use of PETs can keep data securely encrypted in storage, transit, and *in-use* (while being processed), so that sensitive plaintext information is not exposed to third parties who may violate their data-sharing agreement or fiduciary obligations to engage in misconduct. Collaborative information-sharing on advanced privacy-preserving technologies such as MPC and FHE is critical for systemic accountability and data protection.

Clarification 1: Risk Management in Data Processing is Critical to Preventing Data Breaches

The NIST Privacy Framework is structured as an iterative risk management tool to be used in conjunction with the 'Framework for Improving Critical Infrastructure Cybersecurity' ("NIST Cybersecurity Framework").[4] This governance method—chronologically organized as "Core," "Profiles," and "Implementation Tiers," requires businesses to make privacy-driven decisions in activities related to the processing of personal data.

The first pillar—Core—which represents executive priorities and privacy-protective outcomes that guide specific action plans, is subdivided by five functions: Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P. The NIST Privacy Framework explains that "the first four can be used to manage privacy risks arising from data processing, while Protect-P can help organizations manage privacy risks associated with privacy breaches."[5]

Protect-P is defined as developing and implementing appropriate data processing safeguards. The function aims to prevent data breaches with security controls and "protective technology," yet the NIST

---

[3] Yehuda Lindell & Benny Pinkas, *Secure Multiparty Computation for Privacy-Preserving Data Mining*, The Journal of Privacy and Confidentiality (2009), http://jpc.cylab.cmu.edu; *ING Belgium Sees Opportunities for 'Secret' Sharing of Encrypted Data*, The Wall Street Journal (Jun. 1, 2017), https://blogs.wsj.com/cio/2017/06/01/ing-belgium-sees-opportunities-for-secret-sharing-of-encrypted-data/

[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[5] NIST, Preliminary Draft, *NIST Privacy Framework: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT* (Sep. 6, 2019), at 5. https://www.nist.gov/sites/default/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf

Privacy Framework does not directly align this step with instituting PETs in data processing operations. Privacy engineering in data processing, such as employing encryption in-use to secure data in memory while it is being processed, is an essential prerequisite to preventing data breaches. We believe that Protect-P applies to both risk management of data processing and the prevention of unauthorized access—and that both safeguards should be guided by privacy-preserving cryptography.

Clarification 2: Unnecessary Data Transfers Threaten Informational Self-Determination

Privacy harms are contextual and driven by evolving social and technological norms. The NIST Privacy Framework defines privacy risks in data processing as:

> *[R]anging from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm. Problems can arise as unintended consequences from data processing that organizations conduct to meet their mission or business objectives.*
>
> (Page 6, Preliminary Draft of the NIST Privacy Framework)

Unintended inferences and embarrassment are certainly important instances of privacy violations. However, not all privacy harms require detrimental consequences. Informational asymmetries between consumers and companies that undermine consent, or data transfers without sufficient privacy and security safeguards, pose privacy risks even if the resulting harm is not obvious to the individual.

We recommend NIST to engage in a discussion of 'informational self-determination' as a theory underpinning privacy rights and interests. "The right of the individual to decide what information about himself should be communicated to others and under what circumstances"[6] supports the minimization of data collection and transfers to third parties. Privacy-preserving cryptography that eliminates the need to transfer data by maintaining data residency and sovereignty is closely linked to this informational right.

Clarification 3: Encryption in-Use Respects Data Access Controls

The NIST Privacy Framework acknowledges the value of cryptographic PETs in safeguarding privacy values and rights, but caveats that encryption and distributed computing may obstruct data subject access requests:

> *The methods for safeguarding these values may differ, and moreover, may be in tension with each other. For instance, if the organization is trying to achieve privacy by limiting observation, this may lead to implementing measures such as distributed data architectures or privacy-enhancing cryptographic techniques that hide data even from the organization. If the organization is also trying to enable individual control, the measures could conflict. For example, if an individual requests access to data, the organization may not be able to produce the data if the data has been*

[6] Westin, A., *Privacy and Freedom*, New York: Atheneum, 1970.

distributed or encrypted in ways the organization cannot access.

(Page 8, Preliminary Draft of the NIST Privacy Framework)

We wish to clarify two things to address this concern. First, even if cryptographic techniques such as MPC is employed to "limit observation" by computing on private data held by multiple parties without revealing those inputs—each party would still see the headers of the datasets contributed by others. Thus, in the event of a data subject access request by an individual who seeks an explanation of the output, organizations can provide a meaningful overview of the categories of variables that were used in the computing function without knowing the exact value of data. This method would help individuals understand the types of data that were weighed for a decision, whilst also eliminating the organizational risk of fulfilling a data subject access request on the underlying sensitive information without due identity authentication safeguards.[7]

Second, the purpose of cryptographic privacy safeguards is to eliminate the need to transfer data to third parties—against whom consumers have limited to no data subject rights. The status quo of the data ecosystem is that individuals have virtually no knowledge of the secondary processing of their data, or how their personal information gets centralized and exposed to consolidated risk in third-party repositories (i.e. cloud service providers, artificial intelligence models, advertising networks).

PETs that keep data encrypted in-use, or enable distributed computing through MPC, allow knowledge-sharing and collaboration without exposing plaintext personal data to external entities. Inpher has testified to the U.S. House Financial Services Committee on how cryptographic PETs alleviate the privacy and security risks inherent in the centralization of data, in the context of preventing financial data breaches:[8]

> *As banks move more of their data and information processing to the cloud, they are effectively consolidating risk into a select few providers of cloud computing infrastructure. The magnitude of this risk was underscored by the recent Capital One cloud hack.[9] The breach could have been prevented by securely computing across distributed data in a multi-cloud architecture, in which data is processed without exposing the underlying personal information. This would have eliminated a single point of failure.*

---

[7] John Dunn, *GDPR privacy can be defeated using right of access requests*, Naked Security (Aug. 12, 2019), https://nakedsecurity.sophos.com/2019/08/12/gdpr-privacy-can-be-defeated-using-right-of-access-requests/

[8] Inpher, *Inpher CEO Dr. Jordan Brandt testifies before the U.S. House Financial Services Committee on "AI and the Evolution of Cloud Computing"* (Oct. 22, 2019), https://www.inpher.io/news/brandt-testimony-artificial-intelligence-and-cloud-computing; Testimony available here: https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-brandtj-20191018.pdf

[9] Christian Berthelsen, Matt Day, and William Turton, *Capital One Says Breach Hit 100 Million Individuals in U.S.*, Bloomberg (Jul. 29, 2019), https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says

(Oct. 18, 2019, Testimony of Dr. Jordan Brandt before the U.S. House Financial Services Committee, Task Force on Artificial Intelligence)

Moreover, a white paper published by the World Economic Forum entitled 'The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value'[10] details the application of FHE and MPC to limit data transfers to untrusted third parties:

> *If the data steward (data source) does not trust the third party, it will be reluctant to share this data for fear that it will be misused by insiders within the third party or its other partners. Finally, if this third party were to be breached, the original data steward would likely still be held responsible by its customers for sharing the data with the third party in the first place. Homomorphic encryption (HE) can be used to address these challenges by encrypting the data so that analysis can be performed on it, without the information itself ever being readable. The results of the analysis would also not be readable by anyone other than the intended party (usually the owner of the input data).*

As such, individuals retain the power to exercise data subject access and control rights against the primary steward of their information. Encryption in-use is not an obstacle to actionable data subject rights; conversely, it eliminates the risk of data being transferred to a third party where the individual would have no knowledge, control, or access over secondary processing.

Conclusion

Thank you for the opportunity to comment on this important consultation. We support the NIST Privacy Framework as a critical guideline to designing and deploying products and services that will fundamentally prioritize individual privacy.

If you have any questions regarding our comments, or if Inpher could be of any assistance, please do not hesitate to contact me at sunny@inpher.io.

Sincerely,

Sunny Seon Kang
Senior Privacy Counsel, Head of Policy
Inpher, Inc.

[10] World Economic Forum, *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value* (Sep. 12, 2019), https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value