From: Homomorphic Encryption <contact@homomorphicencryption.org>
Sent: Thursday, October 24, 2019 4:10 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Kristin Lauter <klauter@microsoft.com>; Kim Laine <kim.laine@microsoft.com>; krohloff@duality.cloud; rohloff@njit.edu; vinodv@mit.edu; casimir.wierzynski@intel.com
Subject: NIST Privacy Framework: Preliminary Draft Comments

Hello:

On the behalf of the HomomorphicEncryption.org industry consortium for homomorphic encryption, we would like to provide the attached comments on the NIST Privacy Framework preliminary draft.

Thank you for your consideration,

Dr. Kim Laine (Senior Researcher, Microsoft | kim.laine@microsoft.com)
Dr. Kristin Lauter (Partner Research Manager, Microsoft | klauter@microsoft.com)
Dr. Kurt Rohloff (CTO and Co-Founder, Duality Technologies | krohloff@duality.cloud)
Prof. Vinod Vaikuntanathan (Associate Professor, MIT | vinodv@mit.edu)
Dr. Casimir Wierzynski (Senior Director, AI Products Group, Intel | casimir.wierzynski@intel.com)

Dear Privacy Framework Team,

Thank you for the thoughtful effort and thorough work that has resulted in developing and releasing the Privacy Framework draft. The subject is complex and challenging, but critical to address in modern society. The framework captures the essentials of a comprehensive privacy framework, but in flexible form.

We are a US-based subset of privacy and cryptography professionals who have been contributing to an open industry consortium (HomomorphicEncryption.org) to standardize homomorphic encryption protocols and cryptography-based privacy-enhancing technologies. We see homomorphic encryption (also called Fully Homomorphic Encryption or FHE) as an enabling technology for many use-cases of the privacy framework you have developed.

Background and motivation. Homomorphic encryption is a relatively new encryption technology, that allows computations to be performed directly on encrypted data without requiring a decryption key. Multiple open-source implementations of homomorphic encryption are available today.[1]

Homomorphic encryption has found practical application in many industry domains, including:

- Medical applications, such as for privacy-preserving genome-wide associated studies to enable cancer research;
- Financial applications, such as to help financial institutions fight fraud and money laundering;
- Defense industry applications, such as to help identify cyber-attacks.

The UN Global Working Group on Big Data recently released a handbook on privacy-preserving techniques[2] to help national statistics offices collaborate on private statistical data that otherwise could not be shared internationally; homomorphic encryption is one of the core enabling technologies presented in the handbook.

We have also recently seen homomorphic encryption coalesce into higher-level frameworks, such as the Intel nGraph-HE[3] work, and the IARPA-sponsored RAMPARTS and HECTOR activities.

[1] E.g., Microsoft SEAL (https://GitHub.com/Microsoft/SEAL), PALISADE (https://palisade-crypto.org/), HElib (https://github.com/homenc/HElib), HEAAN (https://github.com/snucrypto/HEAAN), Lattigo (https://github.com/ldsec/lattigo)

[2] https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook

[3] https://ngra.ph/he

Our suggestion. We see encrypted computing technologies such as homomorphic encryption to enable end-to-end protection for data during computation, in addition to protecting data-at-rest (PR.DS-P1) and protecting data-in-transit (PR.DS-P2). Therefore, we suggest the addition of a new subcategory to PR.DS: *protecting data-in-use*. This new subcategory would, in most cases, be enabled through access policies, but in some cases though cryptographic technologies such as homomorphic encryption to shift and consolidate the control of the data from the data handlers to the data owners.

Respectfully,

Kim Laine (Senior Researcher, Microsoft | kim.laine@microsoft.com)

Kristin Lauter (Partner Research Manager, Microsoft | klauter@microsoft.com)

Kurt Rohloff (CTO and Co-Founder, Duality Technologies | krohloff@duality.cloud)

Vinod Vaikuntanathan (Associate Professor, MIT | vinodv@mit.edu)

Casimir Wierzynski (Senior Director, AI Products Group, Intel | casimir.wierzynski@intel.com)