From: Vishik, Claire <claire.vishik@intel.com>
Sent: Thursday, October 24, 2019 4:51 PM
To: privacyframework <privacyframework@nist.gov>
Cc: claire.vishik@intel.com
Subject: Intel comments on Preliminary Draft of the NIST Privacy Framework

Dear Naomi and Team,

It was good to read the Preliminary Draft of the NIST Privacy Framework and see how well the initiative is progressing! Attached please find a few Intel comments on the Draft. Please don't hesitate to get in touch if we can clarify any of the comments.

Regards and thanks,

Claire

Claire Vishik. PhD,

Intel Fellow

October 24, 2019

To the NIST Privacy Risk Management Framework Team:

Intel appreciates the opportunity to provide comments on the Draft of the Privacy Risk Management Framework. The comments provided below focus on key technology approaches to enable organizations to adapt to privacy risks arising from emerging technologies, such as artificial intelligence.

Privacy enhancing technologies, e.g., homomorphic encryption and secure multiparty computation, could play a significant role in reducing privacy risks in AI and other data intensive areas. They could be used in addition to ***access control techniques*** for the protection of data in both "Control-P" and "Protect-P" areas.

The discussion on standardization of **homomorphic encryption** and **secure multiparty computation** recently started, e.g., in special interest groups[1] and in ISO/IEC JTC1 SC27.[2] Interest from industry,[3,4,5,6] academia[7,8,9,10,11,12,13] and government[14] in the research in these areas continues to grow, while the performance trade-offs associated with the use of these techniques continue to shrink.

A number of studies and the first products demonstrated the relevance of homomorphic encryption and secure multiparty computation to the field of artificial intelligence, with the applications in finance, healthcare and security, among many other areas. [15]

---

[1] https://homomorphicencryption.org
[2] https://www.iso.org/standard/67740.html
[3] Boemer et al. nGraph-HE: a graph compiler for deep learning on homomorphically encrypted data. *In ACM CF 2019.* (https://github.com/NervanaSystems/he-transformer)
[4] Rosario Cammarota, Indranil Banerjee, and Ofer Rosenberg. 2018. Machine learning IP protection. In Proceedings of the International Conference on Computer-Aided Design (ICCAD '18).
[5] Chandran et al. EzPC: Programmable, Efficient, and Scalable Secure Two-Party Computation. In *IACR Cryptology ePrint Archive*, 2017:1109, 2017.
[6] Lauter. 2017. Microsoft SEAL Library. https://www.microsoft.com/en-us/research/project/microsoft-seal/
[7] Zhu et al. Enabling Privacy-Preserving, Compute-and Data-Intensive Computing using Heterogeneous Trusted Execution Environment. arXiv preprint arXiv:1904.04782.
[8] Juvekar et al. GAZELLE: A Low Latency Framework for Secure Neural Network Inference. *In USENIX Security 2018.*
[9] Büscher et al. HyCC: Compilation of Hybrid Protocols for Practical Secure Computation. *In ACM CCS 2018.* (https://gitlab.com/securityengineering/HyCC)
[10] Demmler et al. ABY – A Framework for Efficient Mixed-Protocol Secure Two-Party Computation. *In NDSS 2015* (https://encrypto.de/code/ABY)
[11] Songhori et al. TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits. *In IEEE S&P 2015.*
[12] Wang et al. ObliVM: A Programming Framework for Secure Computation. *In IEEE S&P 2015.*
[13] Rohloff et al. 2019. Palisade Lattice-Based Cryptography Library. https://git.njit.edu/palisade/PALISADE
[14] https://www.darpa.mil/program/programming-computation-on-encrypted-data
[15] https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook

Intel Corporation
2200 Mission College Blvd
Santa Clara, CA 95054

The growing importance of homomorphic encryption as a key privacy enhancing approach is confirmed by research and trade literature[1-15].

We attach a few concrete comments on the Framework below as well as references informing the earlier sections of this document.

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/ Technical)
1	Intel Corporation		3	90	Executive Summary	The context of “ethical decision making” is not apparent at this point in the document. Even though the meaning of “ethical decision making” is clarified later within a specific example, at this point of the document the text should use a general term, e.g., "decision making."	Replace "ethical decision making" with "decision making."	General
2	Intel Corporation		8	268	1.2.2	The paragraph from line 268 - 277 refers to "methods for safeguarding values" within a privacy context. It continues with "achieving privacy by limiting observation" and continues with mentioning "privacy-enhancing cryptographic techniques." It does not provide more accurate reference to what type of encryption techniques the text refers to.	Elaborate more "methods," and "privacy-enhancing cryptographic techniques," with examples. In reference to “methods,” access control, e.g., via isolation of data and software, can include a reference or an example to secure execution environment (e.g., trusted execution environment.) Such techniques allow to compute on data securely in some contexts and does not necessarily involve cryptography. In reference to "privacy-enhancing techniques," the text can refer to the application of the "state-of-the-art privacy-enhancing cryptographic methods and practices for protecting data in use.” Furthermore, examples of such technologies can be included in the text: “Examples of such technologies include but are not limited to advanced cryptographic techniques such as homomorphic encryption, and secure multiparty computation." to name a few. Other examples specific for protecting data in use can refer to “property-preserving encryption, searchable symmetry encryption and functional encryption.” A brief explanation and references of each cryptographic technique can be added.	Technical
3	Intel Corporation		10	356	2.1	The definition of Control-P does not include an explicit mention to secure execution and the state-of-the-art cryptographic technique and practices.	Please, consider adding subcategories and examples of technologies for data protection of data in use to include the state-of-the-art techniques and practices in privacy-enhancing encryption techniques in addition to access control techniques.	Technical
4	Intel Corporation		10	368	2.1	The definition of Protection-P includes access control techniques but does not include mentions to the state-of-the-art cryptographic technique and practices.	Please, consider adding subcategories and examples of technologies for data protection of data in use to include the state-of-the-art techniques and practices in privacy-enhancing encryption techniques in addition to access control techniques.	Technical

Please do not hesitate to contact us for any clarification. The contact information is listed

Intel Corporation
2200 Mission College Blvd
Santa Clara, CA 95054

below.

Rosario Cammarota
Principal Research Scientist
Intel Corporation
rosario.cammarota@intel.com

Casimir Wierzynski
Senior Director
Intel Corporation
casimir.wierzynski@intel.com

Claire Vishik
Intel Fellow
Intel Corporation
claire.vishik@intel.com

Riccardo Masucci
Global Director of Privacy Policy
Intel Corporation
riccardo.masucci@intel.com

Grace Wei
Director of Global Standards
Intel Corporation
grace.wei@intel.com

Intel Corporation
2200 Mission College Blvd
Santa Clara, CA 95054