European Data Protection Board (EDPB) Public Consultation

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Comments of Inpher, Inc.

As a privacy-enhancing technology company and a stakeholder in this discussion, Inpher appreciates the opportunity to advise the European Data Protection Board (EDPB) on the public consultation regarding 'measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.' We applaud the EDPB for recommending and illustrating the use of Secure Multi-Party Computation as a supplementary measure to the General Data Protection Regulation's (GDPR) Article 46 transfer tools, in light of the additional guarantees for the protection of personal data necessitated by the Schrems II (C-311/18) decision.

Inpher is a U.S. and Swiss-based cryptography and machine-learning company with the conviction that encryption and privacy are foundational to the future of computing and commerce. We apply years of academic research on Fully Homomorphic Encryption (FHE) and Secure Multi-Party Computation (MPC) into the production of privacy-preserving analytics in healthcare, financial services, AI development, and more. Inpher is a vocal stakeholder in shaping policy for privacy-enhancing technologies, and we have consistently advocated for data privacy and consumer protection agencies to impose systemic and technical baselines that standardize privacy-enhancing technologies (PETs).

We strongly support the EDPB's consideration of MPC as an accountability tool for cross-border data transfers involving multiple jurisdictions, and offer our following insights and recommendations:

Secure Multi-Party Computation Protects Data from Exposure in Cross-Border Transfers

The EDPB Recommendations establish a six-part step that data exporters should follow when transferring personal data outside of the European Economic Area (EEA), in accordance with their obligations under the GDPR and the decision of the Court of Justice of the European Union (CJEU) in Schrems II. In this guidance, the use of privacy-enhancing technologies such as MPC are considered at the fourth step; regarding supplementary measures that are required to 'bring the level of protection of the data transferred up to the EU standard of essential equivalence.' Use case 5, 'Split or Multi-Party Processing' in pages 25-26 recommend MPC as a valid supplementary measure.

Cryptographic PETs can indeed prevent the transfer of plaintext personal information to a jurisdiction with potentially inadequate protections for privacy as a fundamental right. MPC transforms personal data into random auxiliary numbers that are deleted after each computing phase, rendering them virtually impossible to intercept and re-identify. This technique curbs the unnecessary collection, sharing, and retention of personal data, and overcomes the vulnerabilities of mainstream anonymization techniques which can subject individuals to the unforeseen risks of third-party data access.

We believe it is important to emphasize the policy goals underpinning MPC as a supplementary measure. Collaborative information-sharing on advanced privacy-preserving technologies such as MPC is critical for systemic accountability and data protection, because:

- Distributed and encrypted computing can make sensitive data points accessible to multiple parties without revealing any identifying information. This prevents the multiplication of data security and privacy risks that follow third-party data transfers.

- After each computing operation, these random auxiliary numbers (also called "triplets") are deleted, thereby minimizing data, imposing a strict purpose limitation, and embodying privacy-by-design standards under Art. 25 of the GDPR.

- Unlike classic anonymization techniques, advanced cryptography can unlock the analysis of sensitive data points with multiple data sources without compromising on accuracy.

- A computing protocol using MPC does not transfer any personal data out of a jurisdiction or even the premises of the data controller and respective processors, thereby facilitating compliant knowledge-sharing whilst eliminating privacy concerns in cross-border environments. This privacy safeguard thus prevents personal data from being transferred and exposed to a jurisdiction without "essentially equivalent" rights and remedies for privacy with regards to the GDPR.

- Public authorities in a third country would not be able to reconstitute the random number triplets used in the decentralized compute. This protects the fundamental rights and freedoms of the data subjects from surveillance and data breach risks.

- By facilitating cross-border analytics without impacting data residency or sovereignty, MPC helps companies navigate the extraterritorial impact of the GDPR, and allows collaboration with firms operating in jurisdictions pending adequacy decisions from the European Commission (GDPR Art. 45).

Technologies like MPC that preserve the privacy of the underlying data are integral to facilitating information flows that can support innovation and widen economic activity on data. In our experience, we found MPC to be an essential safeguard for companies wishing to expand to new markets that have transitory or nascent legal frameworks for data protection, like India and Thailand; as well as the more established jurisdictions with strict data sovereignty requirements, like South Korea.

In line with the EDPB's recommendation in the third step to carefully consider objective factors in assessing a non-EEA (or certified adequate under GDPR Art. 45) country's legislation on public authority access to data, institutions should implement privacy-enhancing technologies as a data firewall in case there is any ambiguity or political uncertainty in national policies. This allows businesses to derive value from data in an uncertain regulatory environment.

Built-In Technical Safeguards Over Paper (Contractual) Safeguards

Cryptographic technologies can protect data at rest, in transit, and *in-use* with mathematical certainty, whereas mere operational policies to monitor consent and authorizations cannot ensure absolute privacy firewalls. As discussed above, MPC allows functions to be performed on encrypted data without revealing the underlying information—thereby instituting an incorruptible *ex ante* privacy safeguard against unauthorized access by intermediaries and third parties.[1] In this system, sensitive plaintext information is never exposed to third parties who may violate their data-sharing agreement or fiduciary obligations to engage in misconduct.

Design-based privacy programs can also correct the longstanding information asymmetry between consumers and businesses. MPC eliminates the need to transfer data to third parties—against whom consumers have limited to no data access rights. The status quo of the data ecosystem is that individuals have 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).[2]

The demands of the GDPR and the CJEU's guidance in Schrems II make it more critical than ever for organizations to implement better technological safeguards and protective measures against data breaches. We urge the EDPB to consider privacy-enhancing technologies not as an afterthought or a supplementary measure to the first three steps of a data exporter's due diligence requirements; but as a default standard for accountability in data transfers. Implementing privacy-by-design should be an iterative task that encourages organizations to map out their business need for information and minimize the use of personal data at all stages of the processing. Even in data transfers within the EEA or with authorized jurisdictions, organizations should consider the use of PETs when practicable to ensure that systemic measures are built in to protect data from unnecessary exposure.

Recommended Wording in Page 26

Use case 5, 'Split or Multi-Party Processing' in pages 25-26 would benefit from the addition of the following:

- In the bullet-point that requires "the algorithm used for the shared computation is secure against active adversaries" in page 26, examine the risk of model inversion attacks in Federated Learning, and the use of MPC as an additional safeguard.

Appendix: Additional Resources on MPC

A. Scientific Journals

[1] 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/

Applying secure multi-party computation to improve collaboration in healthcare cloud, IEEE (2016) Third International Conference on Systems of Collaboration (SysCo), https://ieeexplore.ieee.org/document/7831325

Privacy-Preserving Scoring of Tree Ensembles: A Novel Framework for AI in Healthcare, IEEE (2018) IEEE International Conference on Big Data, https://ieeexplore.ieee.org/abstract/document/8622627

Enabling Analytics on Sensitive Medical Data with Secure Multi-Party Computation, European Federation for Medical Informatics (EFMI) (2018), https://ir.cwi.nl/pub/27706/27706.pdf

MPC compliance with the purpose limitation principle of the GDPR (Section 4.2):

> A first challenge is to make organisations and data subjects willing to share their data. MPC should help with this by helping towards GDPR compliance and reducing the risk of unauthorized data re-use of the data.

MPC meeting anonymization standards of the GDPR (Section 5):

> The GDPR undoubtedly gives rise to several issues related to data processing with privacy-preserving techniques. Anonymisation may be a good strategy to benefit from big data, and to mitigate the data protection risks. It is highly probable that data which are de-identified with application of state-of-the-art PETs will fall outside the scope of the GDPR.

Secure and Efficient Multiparty Computation on Genomic Data, IDEAS '16: Proceedings of the 20th International Database Engineering & Applications Symposium (2016), *https://dl.acm.org/doi/abs/10.1145/2938503.2938507*

Privacy preserving processing of genomic data: A survey, Journal of Biomedical Informatics 56:103-111, 2015, https://doi.org/10.1016/j.jbi.2015.05.022

Secure Multi-Party Computation Grid Logistic Regression (SMAC-GLORE), BMC Med Inform Decis Mak 16, 89 (2016). https://doi.org/10.1186/s12911-016-0316-1

ii. General Real-World Applications of MPC for Statistical Analysis and Machine Learning

Achieving Both Valid and Secure Logistic Regression Analysis on Aggregated Data from Different Private Sources, Journal of Privacy and Confidentiality (2012), https://doi.org/10.29012/jpc.v4i1.617

From Keys to Databases—Real-World Applications of Secure Multi-Party Computation, The Computer Journal, Volume 61, Issue 12 (2018) 1749–1771, https://doi.org/10.1093/comjnl/bxy090

Privacy-Preserving Distributed Linear Regression on High-Dimensional Data, Proceedings on Privacy Enhancing Technologies; (2017) (4):345–364, https://eprint.iacr.org/2016/892.pdf

Students and Taxes: a Privacy-Preserving Study Using Secure Computation, Proceedings on Privacy Enhancing Technologies (2016), https://doi.org/10.1515/popets-2016-0019

- Published case study on the use of MPC for a large-scale privacy-preserving statistical study on real government data in Estonia in 2015. At this time, the Data Protection Directive (95/46/EC)—precursor to the General Data Protection Regulation (GDPR)—applied with commensurate standards on anonymization.

B. Law Review Articles

Peer reviewed, reputable legal publications that examine and advocate for cryptographic privacy-enhancing technologies including MPC:

- *Privacy Substitutes,* Stanford Law Review (2013), 66 Stan. L. Rev. Online 89

> Secure multiparty computation has been implemented in various well-known protocols. The area traces its roots to Andrew Yao's "garbled circuit construction," a piece of "crypto magic" dating to the early 1980s. Researchers have used secure multiparty computation to demonstrate privacy-preserving designs in myriad domains--voting, electronic health systems and personal genetics, and locationbased services, to name just a few.

- *Towards a Modern Approach to Privacy-Aware Government Data Releases,* Berkeley Technology Law Journal (2015), 30 Berkeley Tech. L.J. 1967, at 2027

> Secure multiparty computations are electronic protocols that enable two or more parties to carry out a computation that involves both of their datasets in such a way that no party needs to explicitly hand a dataset to any of the others. Because secure multiparty computation allows for queries to be computed without the need for all data storage to be centralized, it reduces the harm from data breach, and allows computations across parties that do not fully trust each other. In theory, it can be combined with the interactive mechanisms and privacy aware computational methods

- *Law, Technology, and Patient Safety*, DePaul Law Review (2019), 68 DePaul L. Rev. 459 Published case study on a municipal government using MPC to analyze gender wage gaps:

> Web-based secure multi-party computation allows information from multiple submitters to be combined to produce results while ensuring that none of the information can be tracked back to any particular submitter.
>
> Regulators are already making use of this technology in other arenas. In 2014, then Mayor Thomas Menino created the Boston Women's Workforce Council […] Working with researchers, the Council proposed the use of secure multi-party computation to gather the data. Following a pilot run, in 2016, the Council was able to convince 69 Boston employers employing over 112,000 workers to sign on to the Compact and to make their data available for aggregation by the computation program. Unsurprisingly, the invisible data revealed a gender gap. Covering 114 employers and nearly 167,000 workers, the 2017 report revealed not only a gender wage gap but also a race wage gap. **This technology might prove useful in moving us towards the collection of more accurate data on adverse events arising from medical care.**

III. Intergovernmental Organizations

Intergovernmental bodies recognize and recommend MPC and FHE as key privacy-enhancing techniques with growing applications in financial services, healthcare, and other vectors for collaborative data analysis. Currently there is strong support from these institutions to standardize practical applications of MPC and FHE.

A. World Economic Forum

- *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value*, WEF White Paper (2019), http://www3.weforum.org/docs/WEF_Next_Gen_Data_Sharing_Financial_Services.pdf o Examining the application of MPC and FHE for financial institutions; benefits of privacypreserving pilot programs for both industry stakeholders and regulators. Inpher contributed to this report.

B. United Nations

- *UN Handbook on Privacy-Preserving Computation Techniques,* Big Data UN Global Working Group (2019), http://publications.officialstatistics.org/handbooks/privacy-preservingtechniques-handbook/UN%20Handbook%20for%20Privacy-Preserving%20Techniques.pdf o Secure Multi-Party Computation (pp. 20-24) o Fully Homomorphic Encryption (pp. 25-30)

C. European Research Council

Keeping our data safe: the role of multiparty computation, The European Research Council (ERC) Magazine (2018), https://erc.europa.eu/news-events/magazine/keeping-our-data-safe-rolemultiparty-computation

Implementing Multi-Party Computation Technology, European Commission Community Research and Development Information Service (CORDIS) (2016), https://cordis.europa.eu/project/id/690978

IV. Industry and Stakeholder Research Groups

A. The Royal Society, Future of Financial Information Sharing Programme

- *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis,* FFIS (2019), https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologiesreport.pdf?la=en-GB&hash=862C5DE7C8421CD36C105CAE8F812BD0

  MPC can also be used to allow private multi-party machine learning: in this case, different parties send encrypted data to each other and they can train a machine learning model on their combined data, without seeing each other's unencrypted data. This removes the need for a trusted central authority that would perform the computation by pooling together all the data and decrypting it. This also presents the advantage that computation is distributed. The use of MPC can address the problems of 'insecurity' and 'exposure', and the risk of revealing sensitive attributes related to individuals or organisations, in a dataset or output. (p. 38)

  - Homomorphic encryption for NHS data – case study in page 34. This case study shows that cryptographic de-identification techniques are already deployed by major public health institutions, but that FHE alone does not provide the added security of MPC's distributed computing and no-key encryption methods.

B. Future of Privacy Forum

- *Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data,* FPF (2017), https://fpf.org/wp-content/uploads/2017/07/privacy_protective_research_-_facilitating_ethically_responsible_access_to_administrative_data.pdf

Thank you for the opportunity to comment, and we kindly ask that this letter and the attachments be entered into the consultation record for public education purposes.

Sincerely,

Sunny Seon Kang
Senior Privacy Counsel, Head of Policy
Inpher, Inc.
sunny@inpher.io