"AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers"

Task Force on Artificial Intelligence
U.S. House Committee on Financial Services

October 18, 2019, 9:30AM
Room 2128 - House Rayburn Office Building

Testimony of Dr. Jordan Brandt, CEO and Cofounder of Inpher

I. Introduction

Cloud computing and AI are distinct and complementary technologies that offer tremendous economic and consumer benefits. The cloud reduces cost and democratizes access to computational resources, which in turn powers AI to streamline business functions and provide new insights that improve consumer welfare.

II. Issue Statement and Roadmap

The committee has correctly identified that these benefits must be harnessed with proper legislative and technological safeguards for data security and privacy. Whereas cloud computing and AI pose distinct risks, a common theme applies to both; don't put all of your eggs in one basket. The consolidation of sensitive personal information into any individual entity, to be mined by data-hungry AI algorithms, poses significant economic risks[1] and an existential threat to the privacy of our citizens. Fortunately, the emergence of Privacy Enhancing Technologies (PETs), and specifically encryption in-use capabilities, can address the concerns of both cloud data security and privacy in AI.

III. Preventing Data Centralization Risks

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.[2] The breach could have been

[1] IBM, *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years* (Jul. 23, 2019), https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

[2] 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

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.

IV. Application of Encryption in Use

To illustrate how this works, it is important to firstly define the three pillars of encryption, which is the best mathematical safeguard of data:

1. Encryption in-transit (https:)- Secures the transmission between sender and receiver.
2. Encryption at-rest (AES)- Secures data storage while on a hard disk.
3. Encryption in-use (Homomorphic Encryption, Multiparty Computation)- Secures data in memory while being processed.

In-transit and at-rest encryption are already ubiquitous. Encryption in-use is rapidly evolving from academic research into practical applications today, as its computing performance for large datasets quantifiably improves.

V. Privacy-Enhancing Technologies: Use Cases and Value

For example, at Inpher, we have made multiple order-of-magnitude improvements in the performance of both Homomorphic Encryption and Multiparty Computation without compromising accuracy. We are currently deploying this technology to solve real-world privacy and security challenges in banking, defense, healthcare, and other industries.[3]

Our platform keeps data private, secure, and resident-- precluding the need to centralize information into a single repository. This proactive safeguard enables financial institutions to minimize risk and leverage the full benefits of AI without a privacy tradeoff. PETs thus internalize the letter and the spirit of U.S. and international data privacy regimes which jointly emphasize privacy-by-design.[4]

Specifically, in the financial services sector, we are witnessing the application of PETs in: fraud and anti-money laundering, credit scoring, trade surveillance, and all forms of predictive modeling where compliant data sharing is critical.

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

[4] Notable international bodies including the United Nations (“UN”), Organization for Economic Co-operation and Development (“OECD”), European Data Protection Board (“EDPB”), and European Union Agency for Cybersecurity (“ENISA”) have all promoted the implementation of PETs to minimize risks to privacy and data protection.

PETs safely overcome data silos and increase data utility. Regulators and law enforcement also benefit from privacy-preserving computing, as they are able to run forensics and surveillance on encrypted data for pattern matching and event detection without compromising individual privacy, or inviting potential liability. They can find the bad guys without compromising honest citizens. To this end we have briefed many domestic and international regulators about these capabilities over the last year and we are encouraged by their enthusiastic support.[5]

VI. Conclusion

To conclude, as a nation, we are in a technology arms race with countries like China that do not share our views on individual rights. We must not accept the false dichotomy between AI and our privacy; we can have both. Privacy-preserving computing not only champions and achieves this outcome, but also fosters new innovation and economic expansion that benefits our government, industry, and every American citizen.

We truly appreciate your interest and desire to learn more about these complex topics, and we remain at your disposal for any further questions you may have.

[5] Inpher, *Inpher Wins People's Choice Award at FCA TechSprint* (Aug. 9, 2019), https://www.inpher.io/news/2019/8/9/inpher-wins-peoples-choice-award-at-financial-conduct-authoritys-2019-tech-sprint.