iapp

A Privacy Enhancing Technologies Primer

Tuesday, 15 September
08:00-09:00 PST
11:00-12:00 EST
17:00-18:00 CET

Welcomes and Introductions

Dylan Gilbert

Senior Fellow for Privacy Engineering

IAPP

Kristie Chon Flynn

Group Data Protection Officer

Google

Curtis Mitchell, CIPT

Principal

Mitchell Technology Consulting

Matthew Reisman

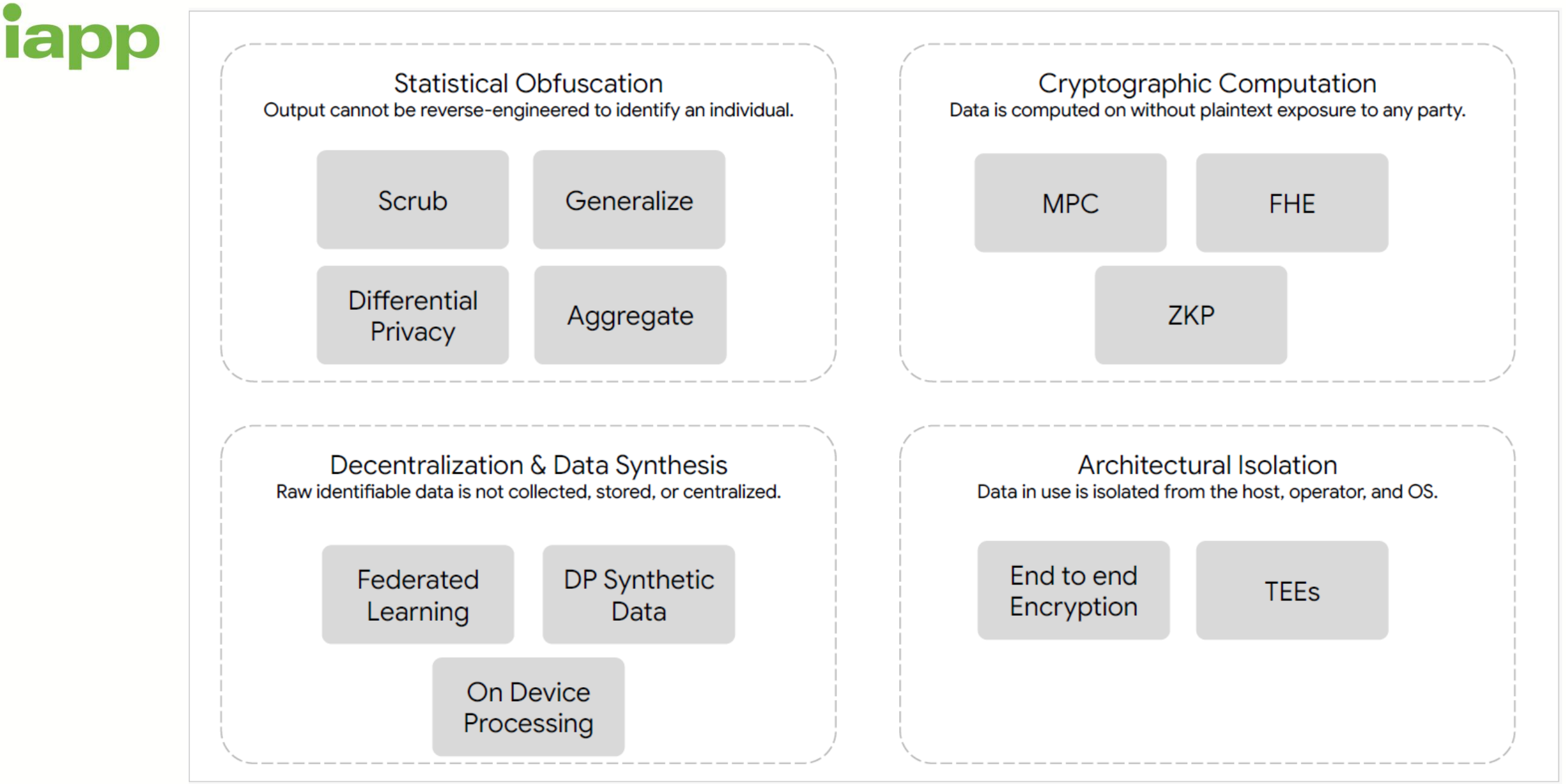
Vice President, U.S. Policy

Future of Privacy Forum

Session Outline

- What are Privacy-Enhancing Technologies?
- Why PETs? And Why Now?
- Considerations for Use
- What the Future Holds
- Q&A

What are Privacy-Enhancing Technologies?


Statistical Obfuscation
Output cannot be reverse-engineered to identify an individual.
Scrub
Generalize
Differential Privacy
Aggregate
Cryptographic Computation
Data is computed on without plaintext exposure to any party.
MPC
FHE
ZKP
Decentralization & Data Synthesis
Raw identifiable data is not collected, stored, or centralized.
Federated Learning
DP Synthetic Data
On Device Processing
Architectural Isolation
Data in use is isolated from the host, operator, and OS.
End to end Encryption
TEEs

Use Cases	Examples	PETs
Generating aggregate insights	• Macro-level insights from end-of-life data • Popularity and busyness insights on Google maps	Differential Privacy
Cryptographic analysis on sensitive data	• Combating financial fraud across jurisdictions • Combating email spam • Age assurance using digital wallets	(Fully) Homomorphic Encryption Federated learning Zero Knowledge Proof
AI model training and inference	• Privacy-preserving federated learning for genomics data • Confidential compute for AI	Federated learning Trusted Execution Environment DP Synthetic data

Why PETs? And why now?

Considerations for Use

What the Future Holds

Audience Q&A