

PrivApprox

Privacy-Preserving Stream Analytics

<https://privapprox.github.io>

[USENIX ATC'17]

Do Le Quoc, Martin Beck,

Pramod Bhatotia, Ruichuan Chen, Christof Fetzer, Thorsten Strufe

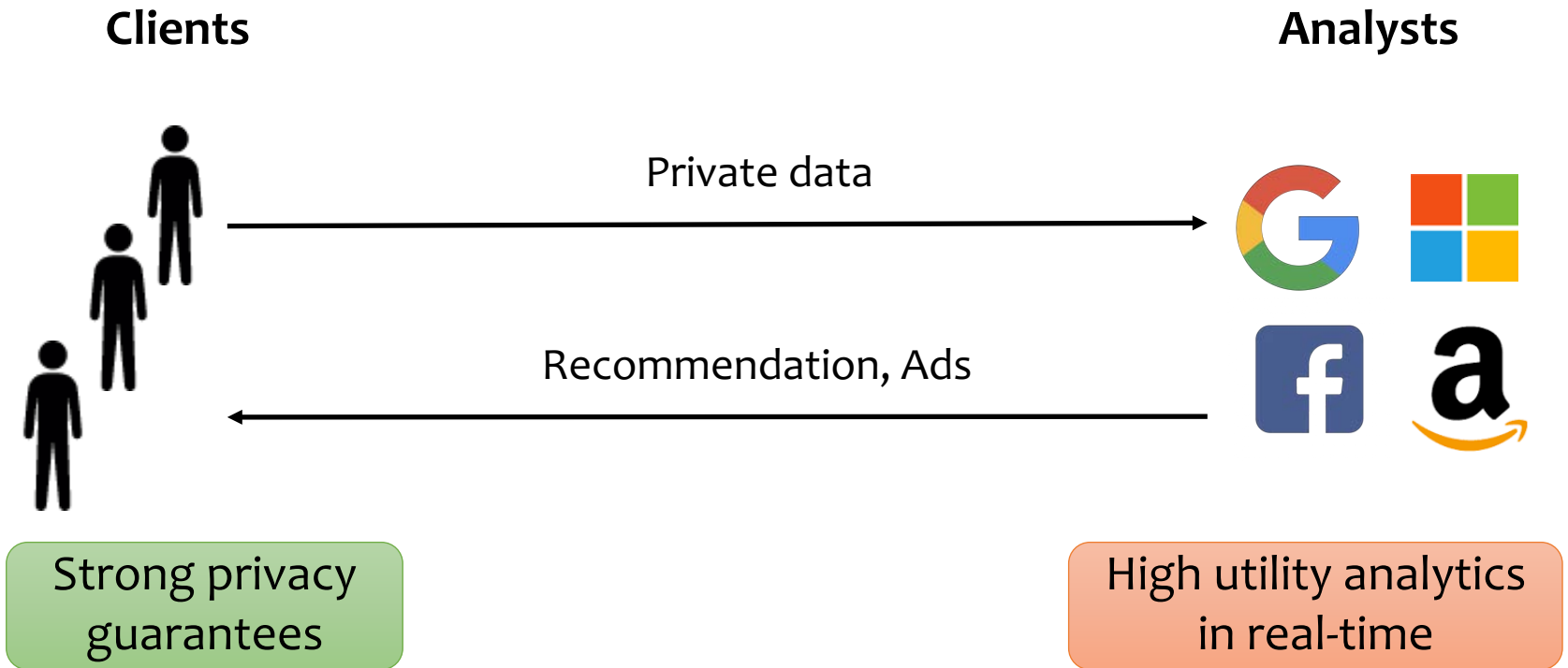


THE UNIVERSITY
of EDINBURGH

NOKIA Bell Labs

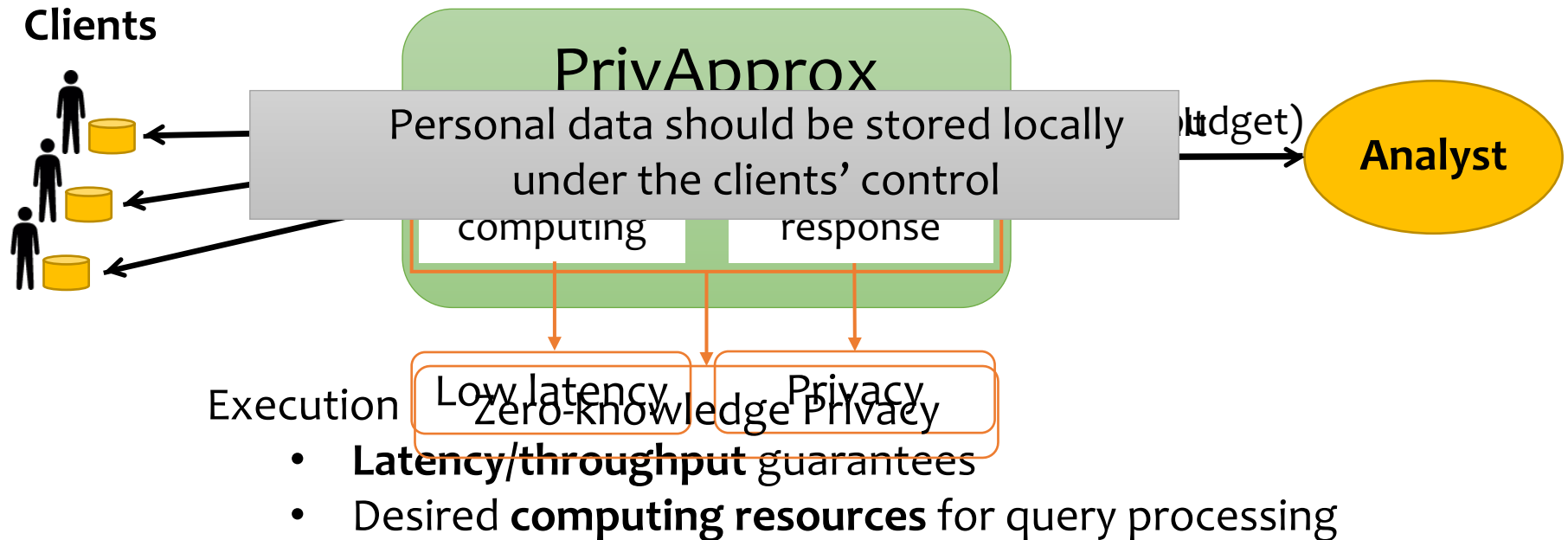
July 2017

Motivation



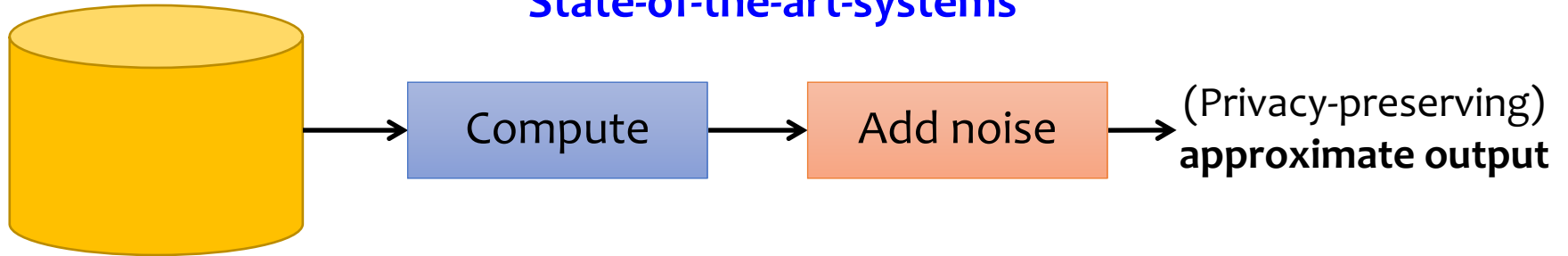
How to preserve users' **privacy** while supporting **high-utility** data analytics for **low-latency** stream processing?

PrivApprox



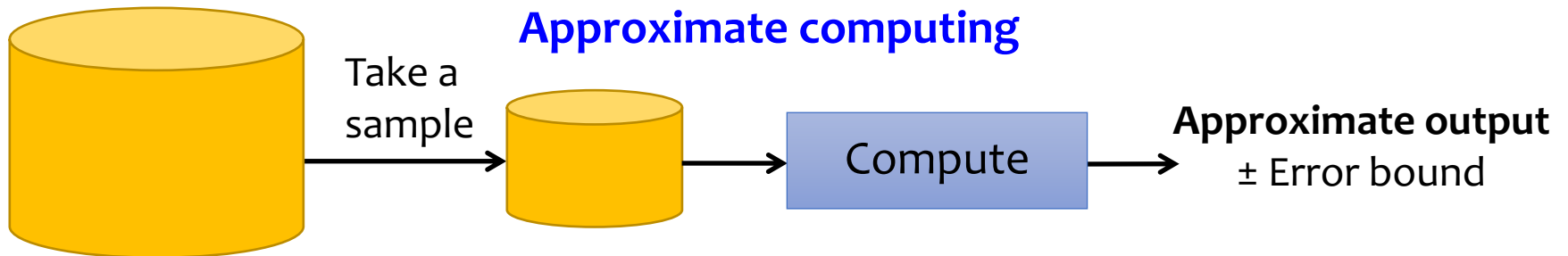
#1: Approximate computing

State-of-the-art-systems



Idea: To achieve low latency, compute over a sub-set of data items instead of the entire data-set

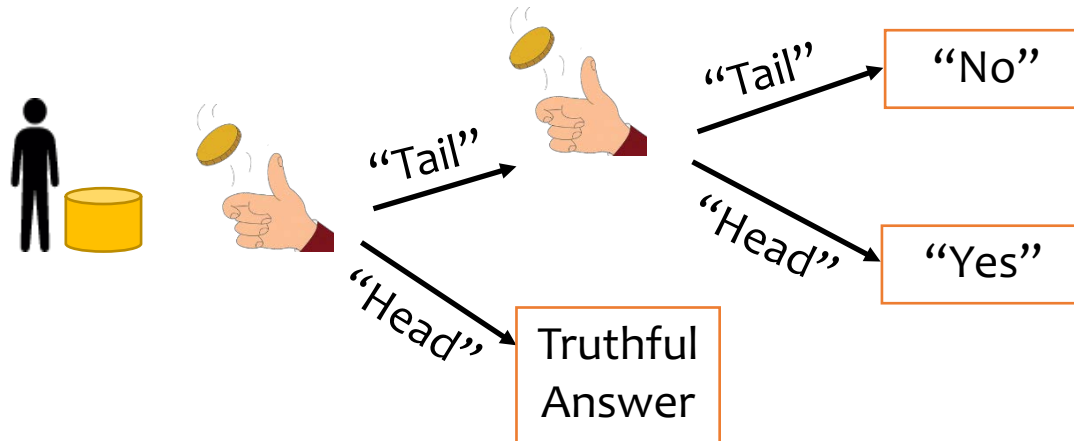
Approximate computing



#2: Randomized response

Idea: To preserve privacy, clients may not provide **truthful answers** all the time

Client



Provides **plausible deniability** for clients responding to sensitive queries; achieves **differential privacy** (RAPPOR [CCS'14])

Summary

PrivApprox: a privacy-preserving stream analytics system over distributed datasets

Privacy

Zero-knowledge privacy

Practical

Adaptive execution based on query budget

Efficient

Randomized response & sampling techniques

Thank you!

<https://privapprox.github.io>