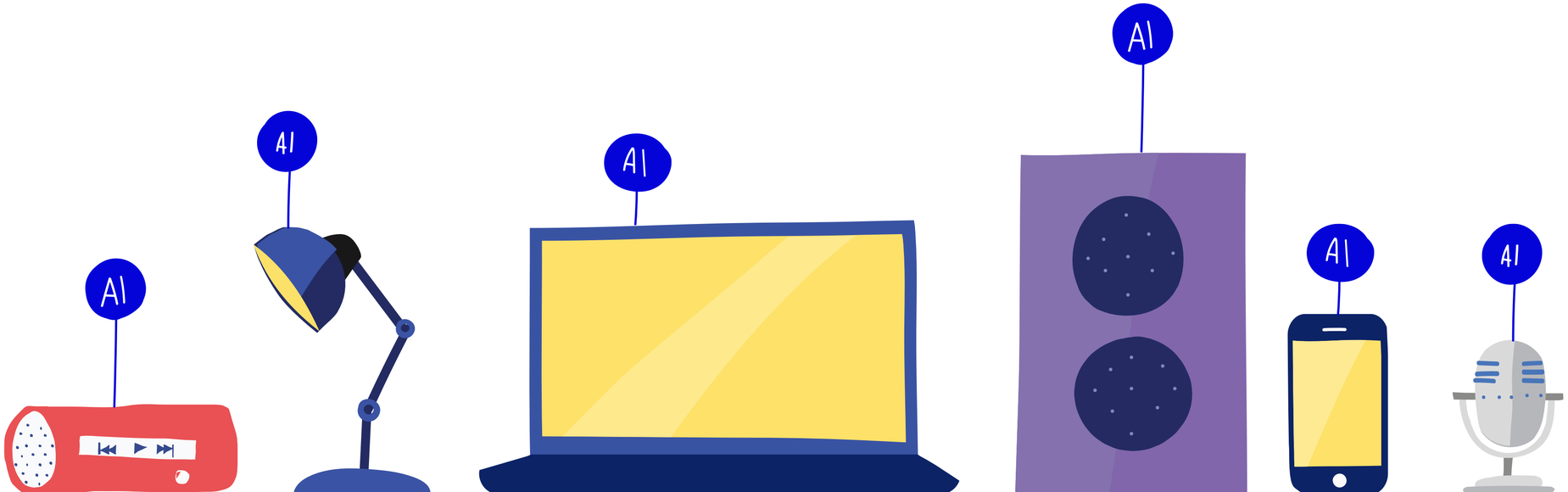
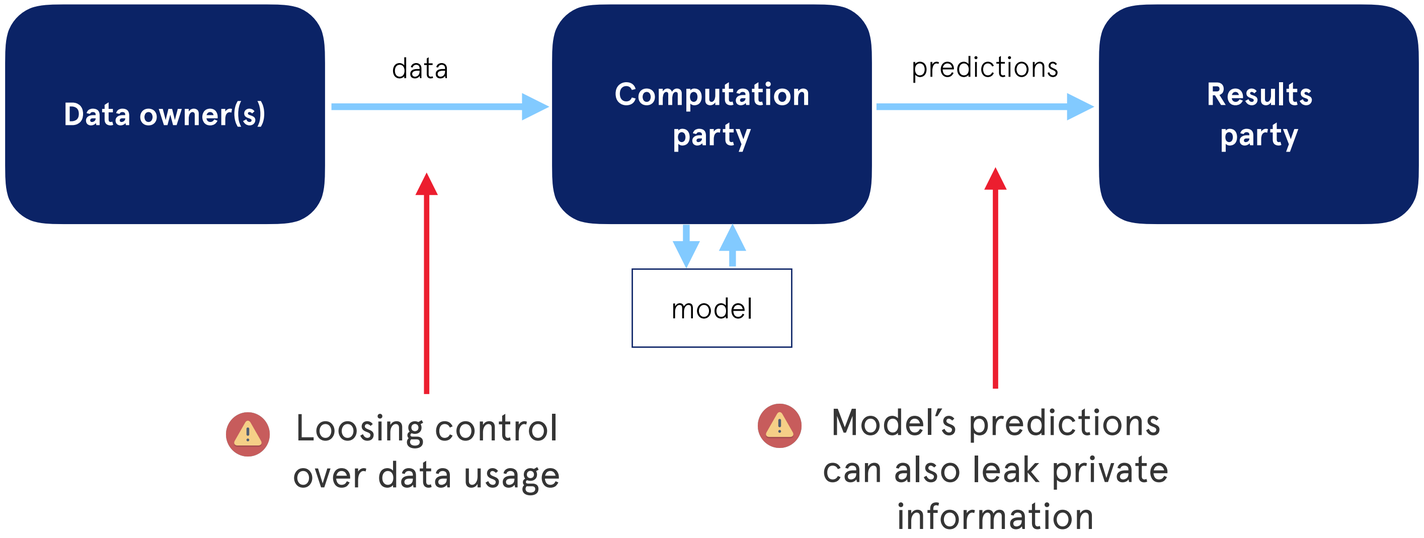
AML19: AI & Privacy

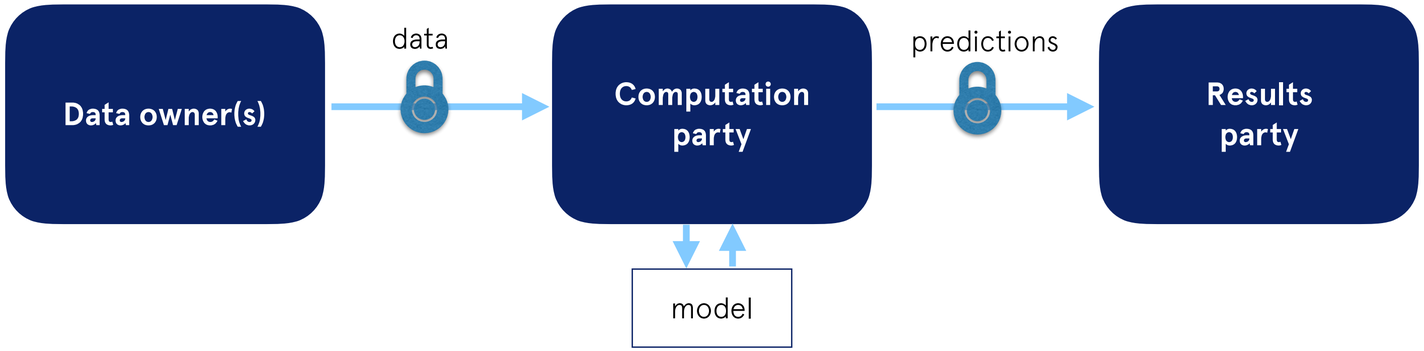
David Leroy, Snips
Jan 28th, 2018



AI & Privacy : the Machine Learning system standpoint



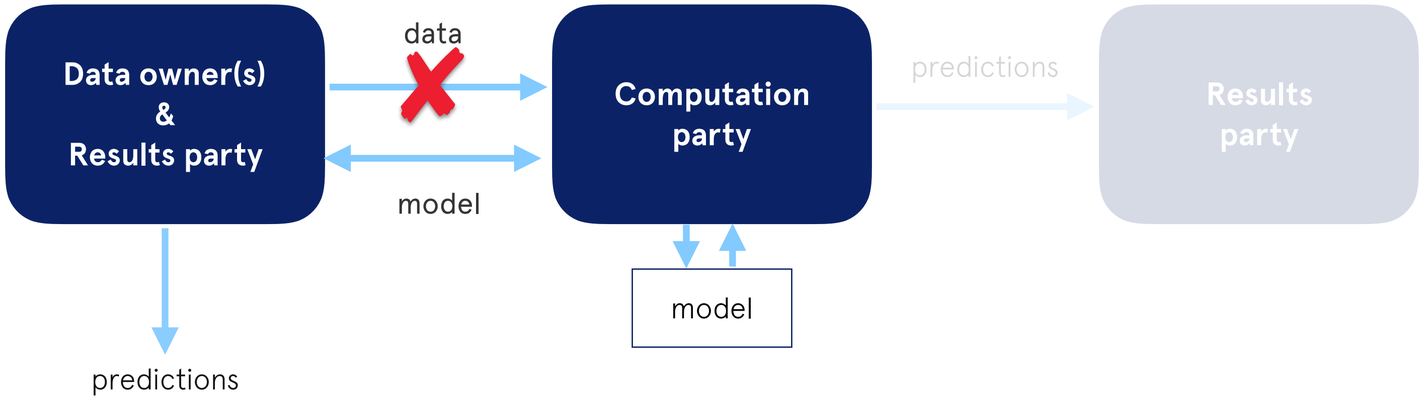
The cryptographic toolbox

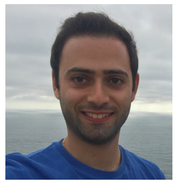


Morten Dahl
Dropout Labs
@motendahlcs

Cryptography for privacy preserving machine learning

Learning a model from decentralized data

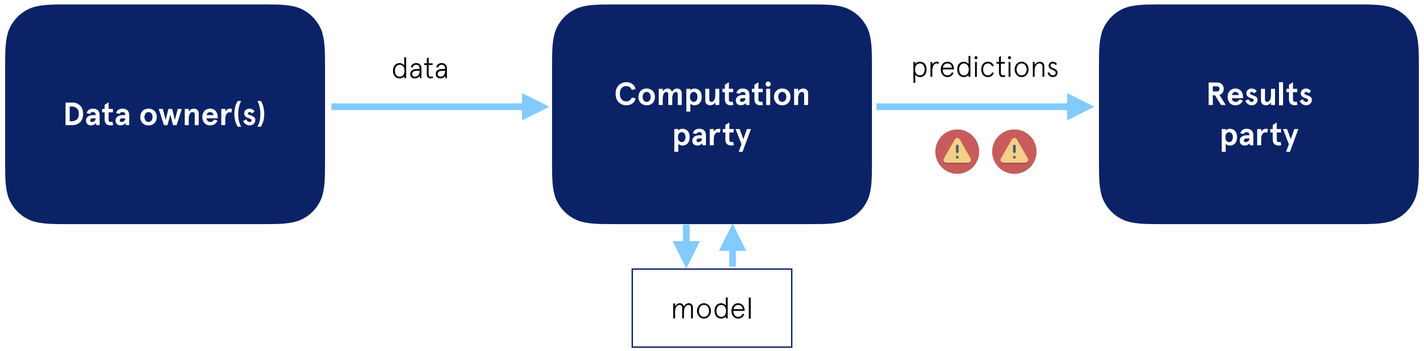




Peter Kairouz
Google

Federated learning
in practice at Google

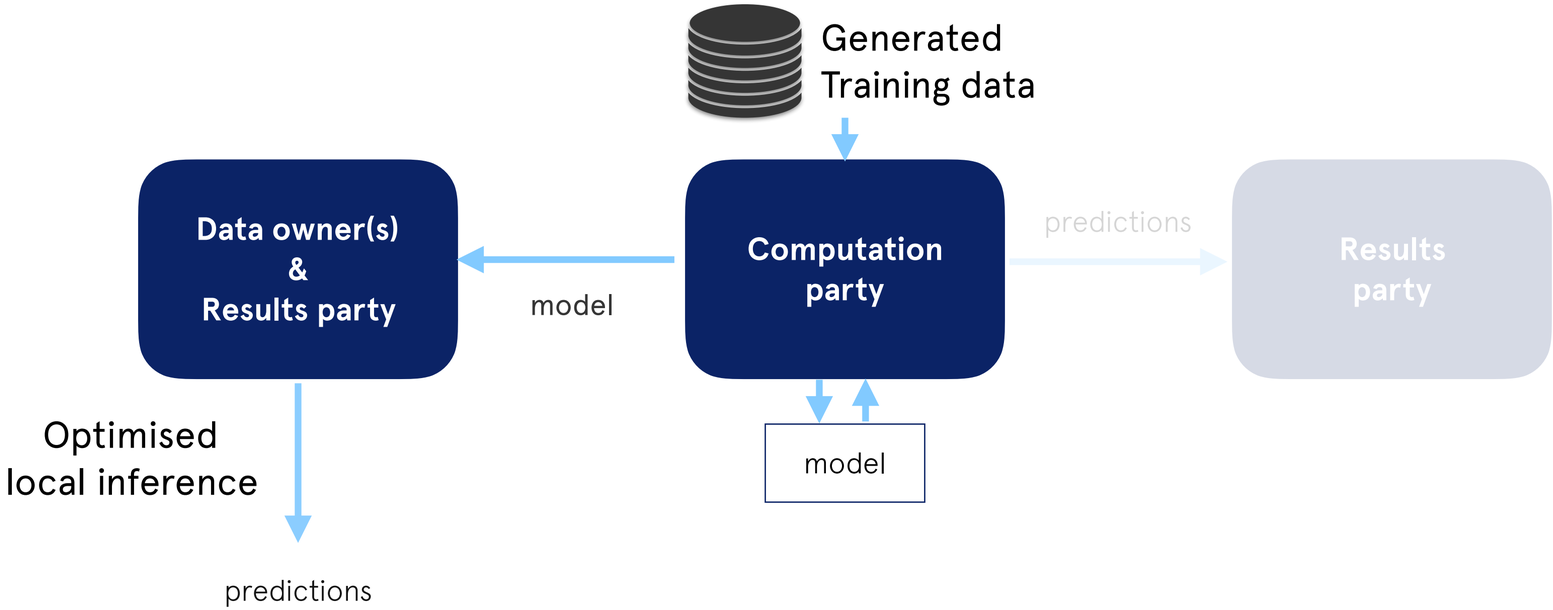
Adversarial examples to the rescue ?



Carmela Troncoso
EPFL, SPRING Lab
@carmelatroncoso

When foes are friends: a privacy perspective on adversarial examples

Voice assistants on the edge



Alice Coucke
Snips
@alicecoucke

Spoken Language Understanding
on the edge