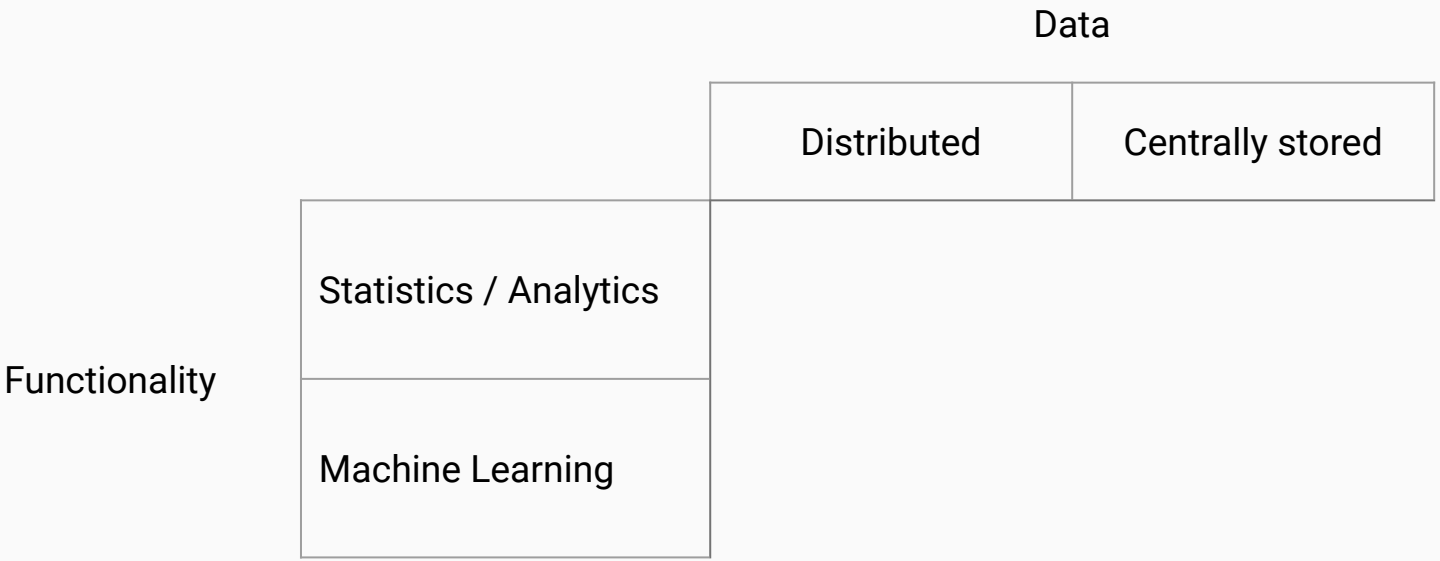
Differential Privacy in the Industry: Challenges and Successes

Ilya Mironov

Modalities of Privacy



Modalities of Privacy

		Data	
		Distributed	Centrally stored
Functionality	Statistics / Analytics	RAPPOR / Cobalt	PINQ
	Machine Learning	Federated Learning	tensorflow/privacy

Modalities of Privacy

Functionality	Data: Distributed	Data: Centrally stored
Statistics / Analytics	RAPPOR / Cobalt	PINQ
Machine Learning	Federated Learning	tensorflow/privacy

Distributed Analytics

Functionality	Data: Distributed	Data: Centrally stored
Statistics / Analytics	RAPPOR / Cobalt	PINQ
Machine Learning	Federated Learning	tensorflow/privacy

Distributed Analytics

- Google Chrome's RAPPOR (2014 – 2019)
  - Based on randomized response
  - Supported more than 200 metrics
- Inspired plenty of follow-up in theory and applications
- Main challenges
  - Utility (absolute error $\sim N^{1/2}$)
  - Privacy loss over time

Distributed Analytics

- Fuchsia OS' Cobalt (in development)
  - Based on randomized response + anonymization channel
- Interesting theory work
- Main challenge
  - Who is doing anonymization?

Analytics over Collected Data

Data

Functionality	Distributed	Centrally stored
Statistics / Analytics	RAPPOR / Cobalt	PINQ
Machine Learning	Federated Learning	tensorflow/privacy

Analytics over Collected Data

- The “standard” setting for differential privacy:
  - McSherry’s PINQ (2009),..., Uber’s Flex (2018)
  - US Census Bureau
- Main challenges:
  - Mission creep
  - Business imperatives
  - Who is keeping the budget?

Differentially private ML

Data

Functionality	Distributed	Centrally stored
Statistics / Analytics	RAPPOR / Cobalt	PINQ
Machine Learning	Federated Learning	tensorflow/privacy

Differentially Private ML

- Two main approaches: PATE and DP-SGD
- DP-SGD is a better fit for standard ML pipeline
- TensorFlow implementation: 800+ stars, 100+ forks
- Challenges:
  - Slower!
  - Learning to learn **with privacy**

References

RAPPOR

"RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response", Erlingsson, Pihur, Korolova, ACM CCS 2014

Shuffle Model

"Prochlo: Strong Privacy for Analytics in the Crowd", Bittau et al., SOSP 2017

PATE:

"Semi-supervised Knowledge Transfer for Deep Learning from Private Training Data", Papernot et al., ICLR 2017

DP-SGD:

"Deep Learning with Differential Privacy", Abadi et al., ACM CCS 2016