**Enhancing Data Privacy through Federated (Machine) Learning**

***Talk outline***

INTRODUCTION

* About me
* About the talk (why is this important/relevant?) (T&C, app permissions, GPS, shared resources, cloud storage, laws (uruguay)…)

DATA PRIVACY

* What is?
* DP in a ML/DL context
* Differential Privacy (overview)
* Evaluating privacy for a function
* Common approaches (and its drawbacks)(anonymized data warehouse/lake, crypto encoding, on-device modelling...)
* So, how to handle this?

FEDERATED LEARNING

* What is?
* How it works?
* Introducing Remote Arithmetic
* Federated vs Distributed vs Multi-Party
* Securing Federated Learning
* Where can we see it in action? (autocomplete, Graph-theoretic Analysis of opinion dynamics - César)

FEDERATED LEARNING IN PYTHON

* Civil War picture (PyTorch vs TF)
* PySyft (OpenMined)
* TensorFlow Federated (Google)
* [FATE](https://pythonawesome.com/an-industrial-level-federated-learning-framework/) (Webank)

DEMO

* Basic FL example with PySyft