Our work w/ aggregate location time-series

1. Mobility analytics using aggregate locations [1]

2. Quantify how much privacy do aggregates leak? [2]

3. Membership inference attacks users contributing to aggregates [3]

[1] A. Pyrgelis, G. Ross, E. De Cristofaro. Privacy-Friendly Mobility Analytics using Aggregate Location Data. In ACM SIGSPATIAL 2016

[2] A. Pyrgelis, C. Troncoso, E. De Cristofaro. What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy. In PETS 2017

[3] A. Pyrgelis, C. Troncoso, E. De Cristofaro. Knock Knock, Who's There? Membership Inference on Aggregate Location Data. In NDSS 2018. Distinguished Paper Award.

Agenda

1. Training (Distributed) ML Models with Privacy

2. Private Data Release with Generative Neural Networks

3. Privacy Leakage from Generative Models as a Service

4. Privacy Leakage in Collaborative/Federate ML