A Unified Framework for IoT Privacy (CNS-1739462, 9/1/2017-8/31/2021)

Hossein Pishro-Nik (PI), Dennis Goeckel (Co-PI), Amir Houmansadr (Co-PI)

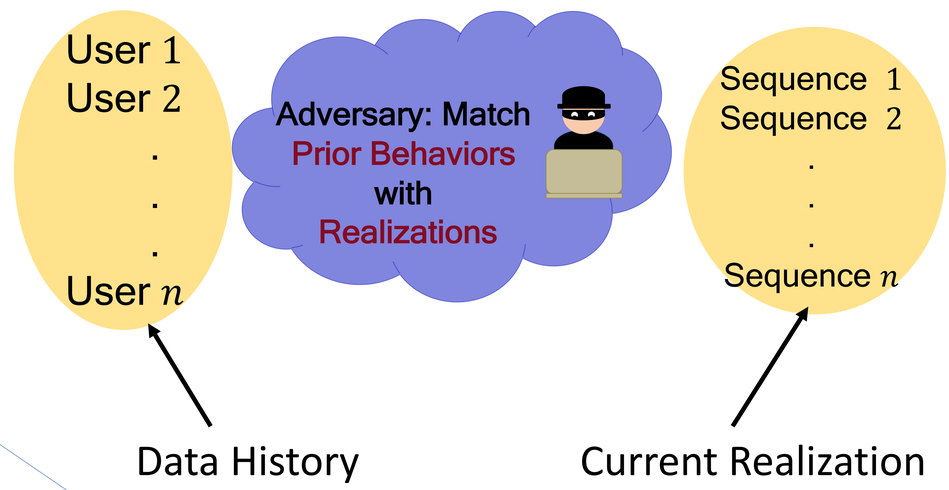
University of Massachusetts - Amherst

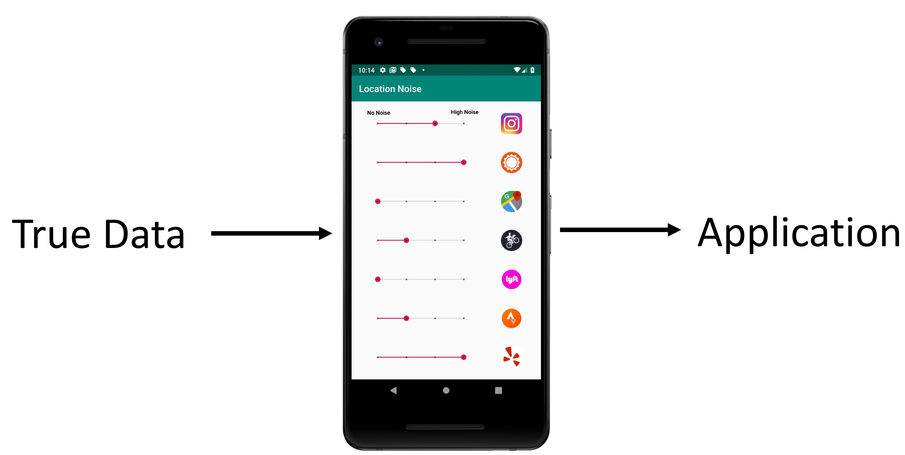
Challenge:

- IoT users gain significant *utility* by sharing data with applications
- Such sharing can compromise our *privacy*

Solution:

- Study methods and utility loss required for *perfect privacy* (no information leakage)
- Results:
  - Degree of anonymization or obfuscation required
  - Novel methods for thwarting pattern matching attacks





Sample Usage: Tunable Obfuscation App

Scientific Impact:

- Provide a framework to protect against information leakage via statistical matching
- Demonstrate challenges of privacy, particularly for dependent users.
- Establish a new framework for privacy against pattern-matching attacks.

Broader Impact:

- App being developed by UMass undergrads for tunable obfuscation for different applications
- Supported multiple Ph.D. students, one now at QualComm, and undergraduate students in paper authorship.
- PI Pishro-Nik a leader in supporting open access content (undergraduate probability text).

University of Massachusetts – Amherst

Hossein Pishro-Nik (pishro@ecs.umass.edu)

Dennis Goeckel (goeckel@ecs.umass.edu)

Amir Houmansadr (amir@cs.umass.edu)