Computational Location Privacy: Two Fundamental Problems

Reza Shokri

ETH Zurich

Department of Computer Science

They Profile You!

Location-based Services

foursquare
Google latitude
WNM LIVE
街旁

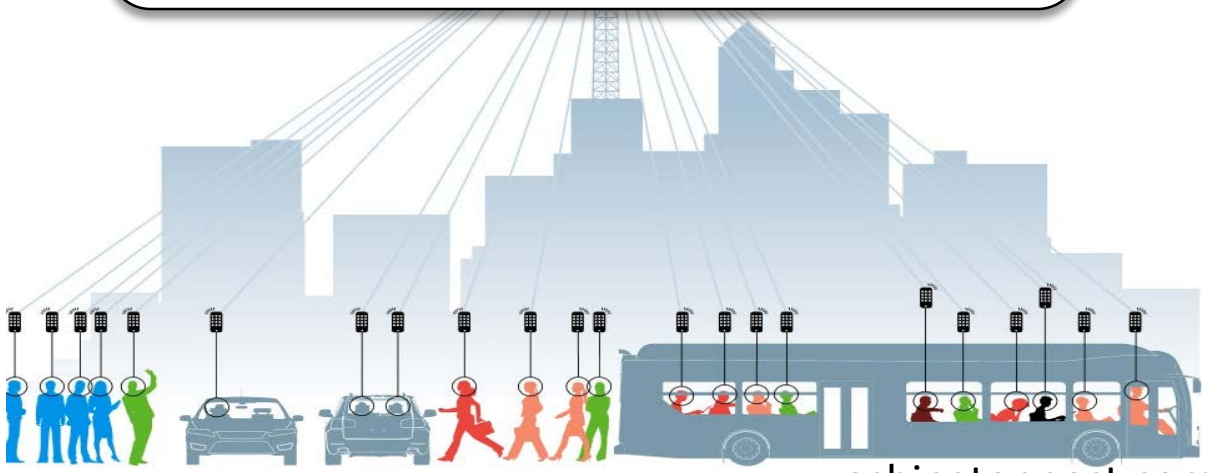
Social Networks

LinkedIn
flickr
Instagram

They Track You!

NSA Location Tracking Programs

- Co-Traveler
- HappyFoot



washingtonpost.com

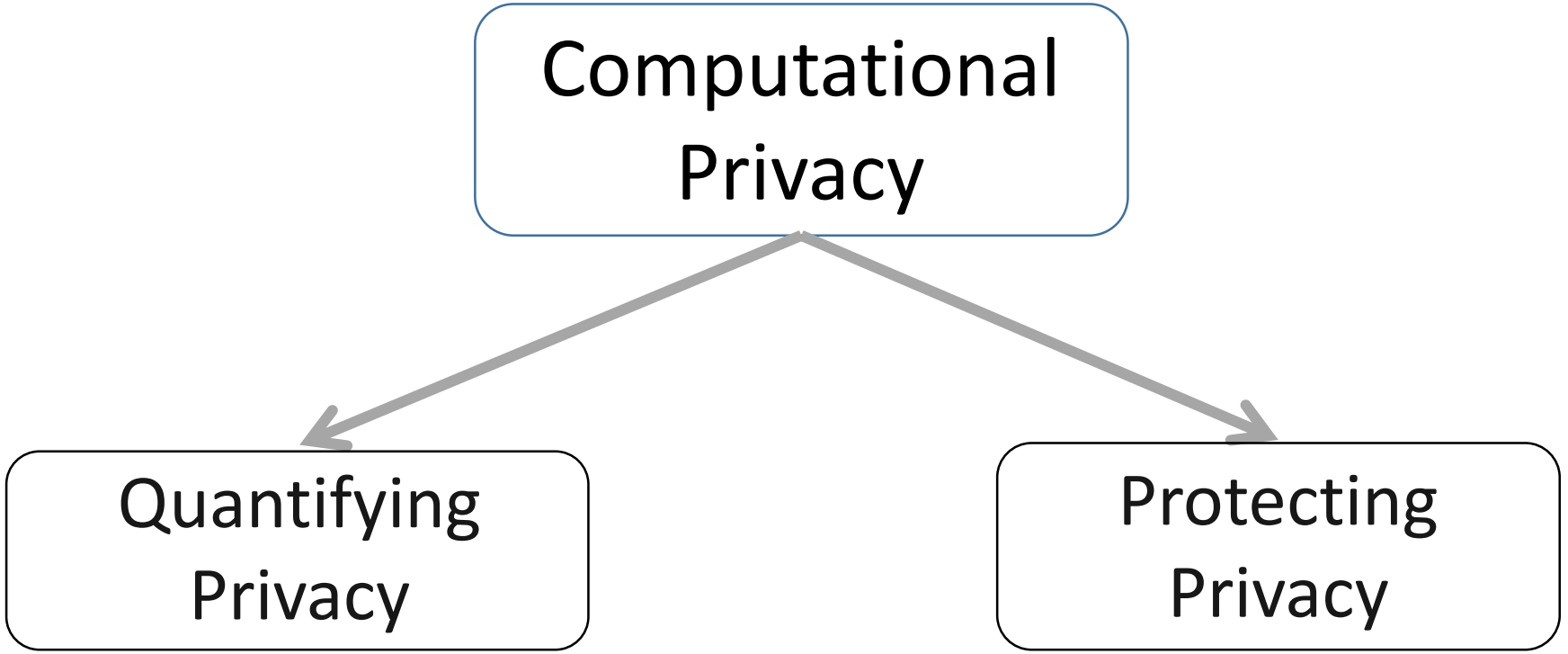
NSA collects 5 billion location records a day on cellphones

Different Approaches to Privacy

Legal

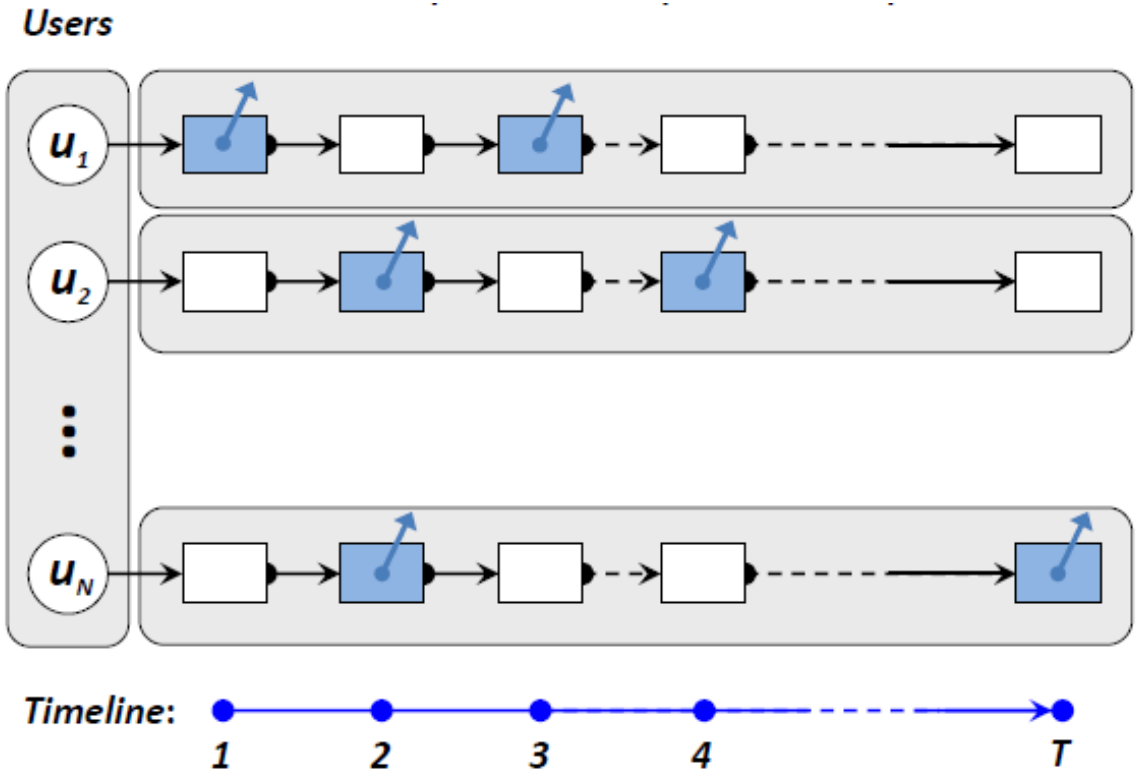
Behavioral

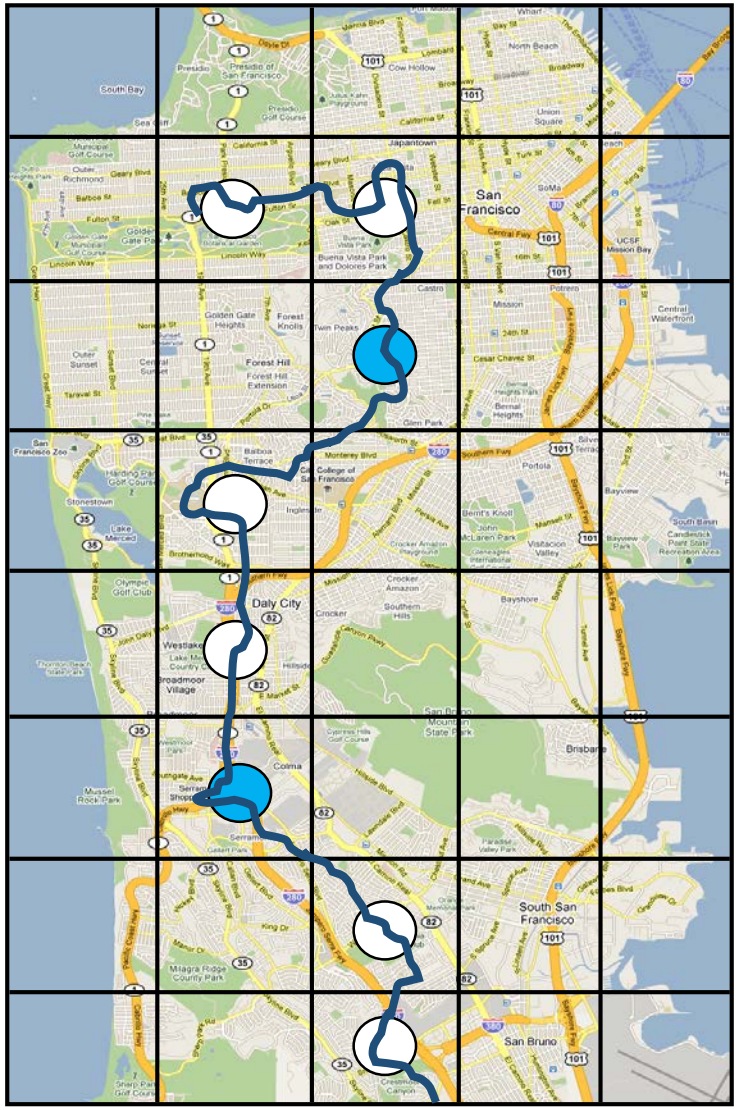
Computational


Computational Privacy
Quantifying Privacy
Protecting Privacy

Location Traces and Location-based Services

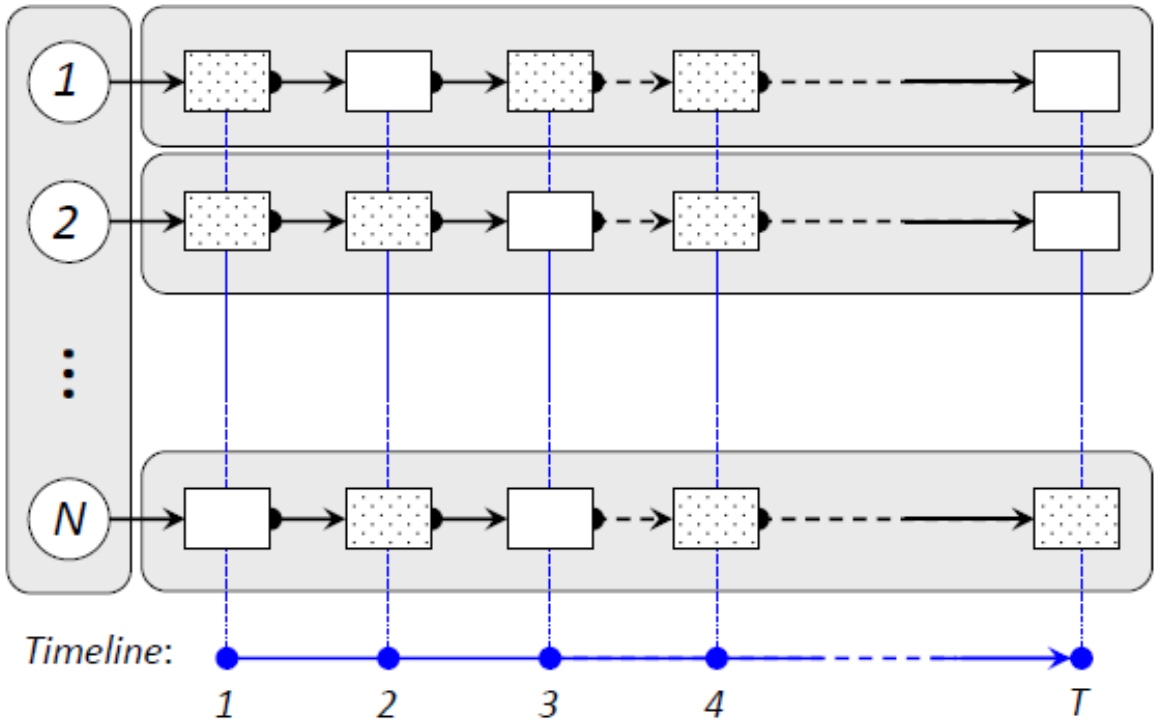
Actual Traces

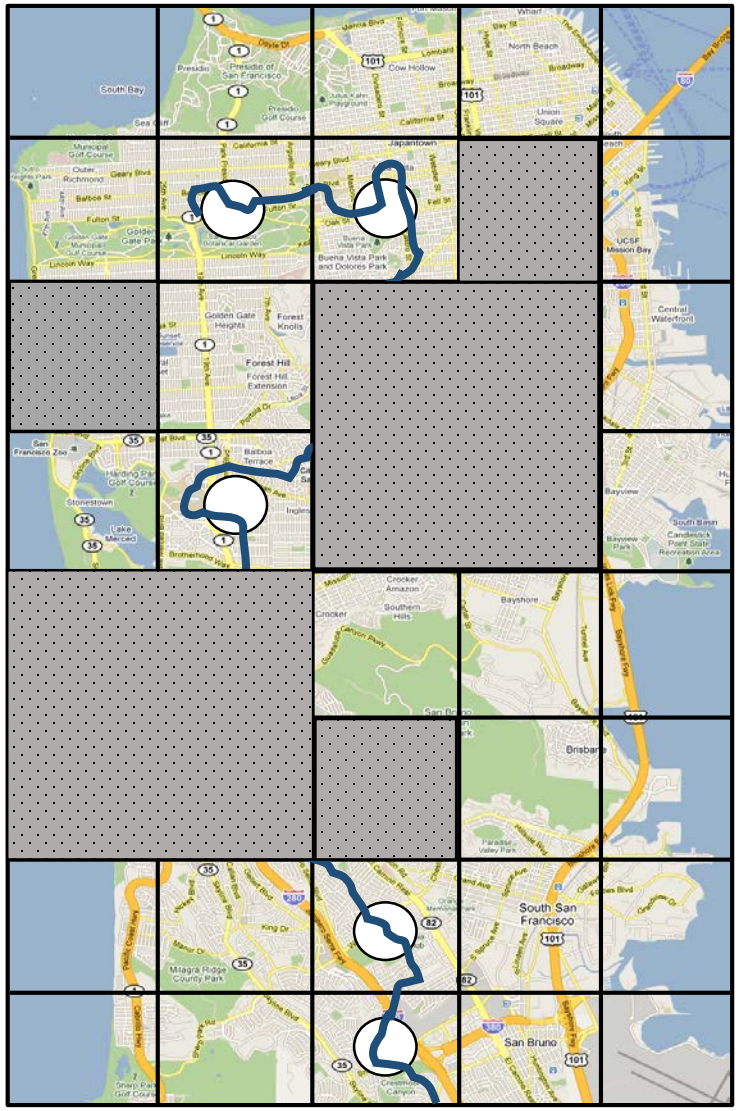




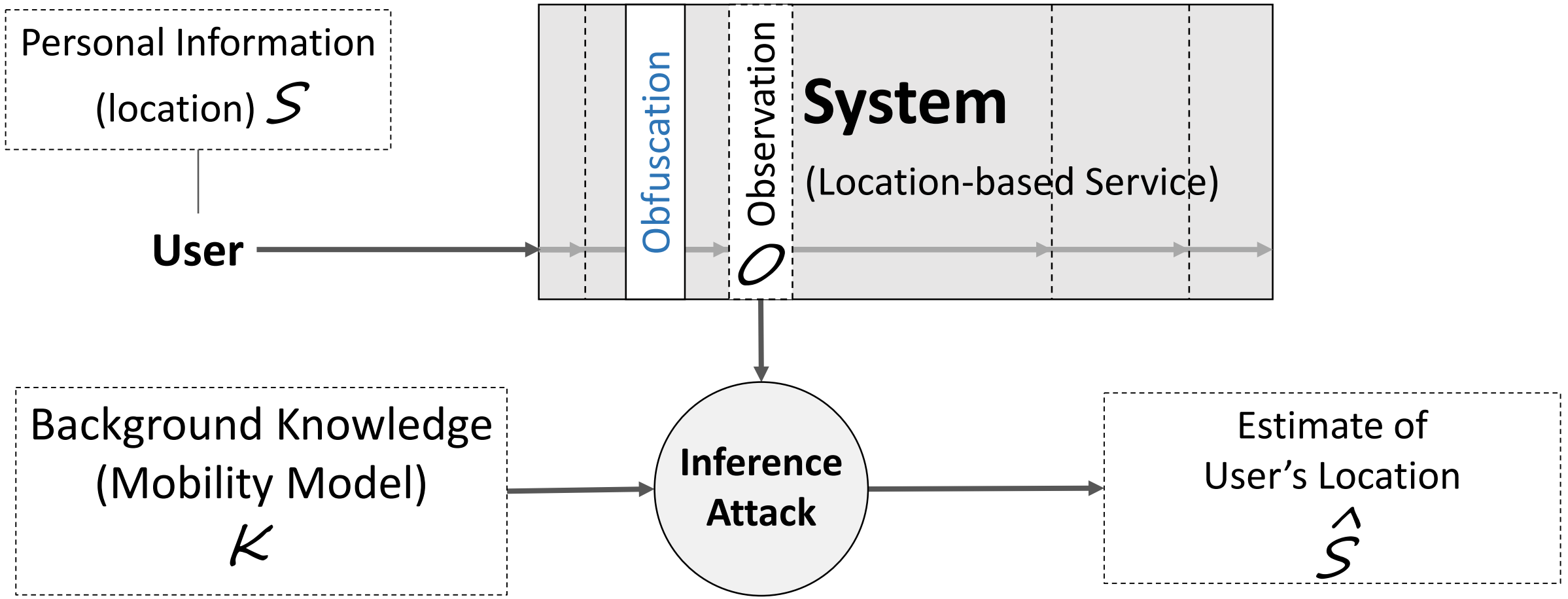
User-Centric Protection Mechanisms

- Anonymization
- Location Obfuscation
  - Decrease Granularity (Location Cloaking)
  - Decrease Accuracy (Location Perturbation)





How to Consistently **Quantify** Location Privacy?



Privacy (as expected inference error): $\sum_{\hat{S}} \Pr(\hat{S} \mid O, K) \cdot d(S, \hat{S})$

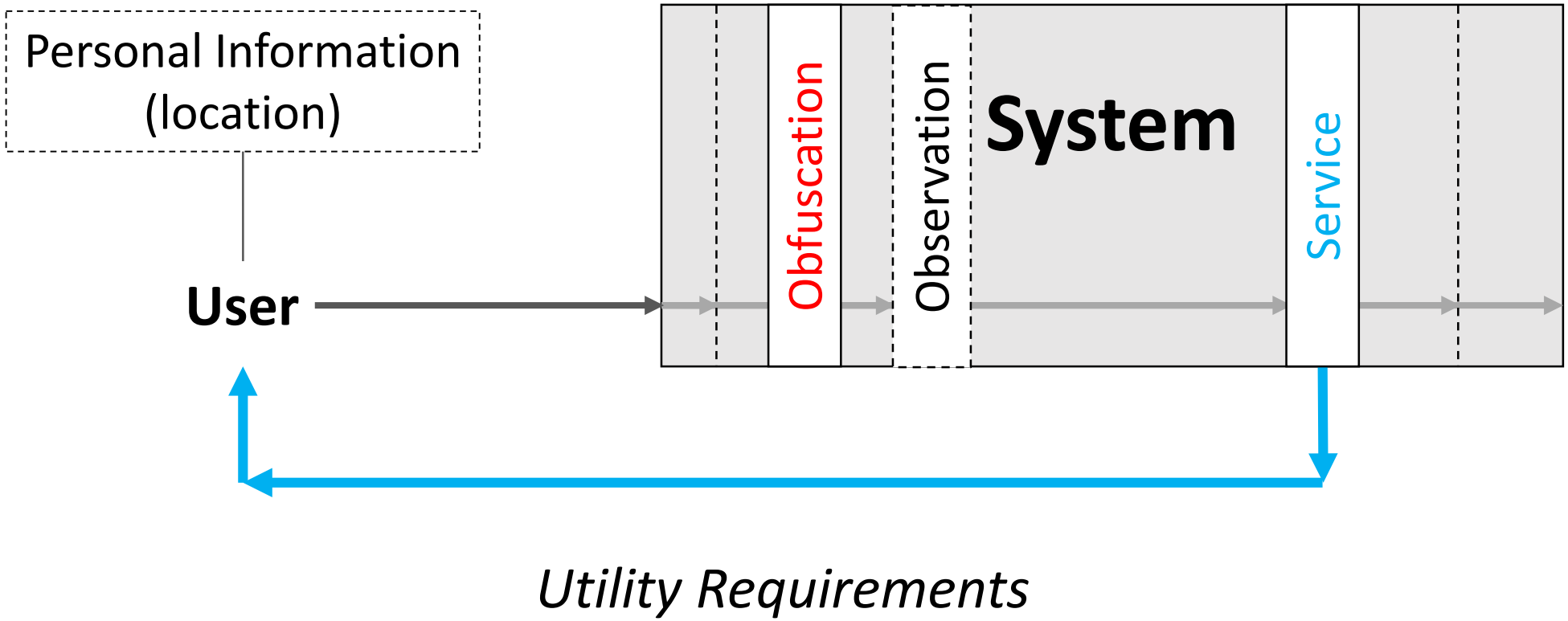
- R. Shokri, et al., "Quantifying Location Privacy," IEEE S&P - Oakland, 2011.
- R. Shokri, et al., "Quantifying Location Privacy: The Case of Sporadic Location Exposure," PETS, 2011.

Inference Attacks

- **Identification:** Which trace does belong to Alice?
- **Localization**: Where was Alice at 8:00?
- **Tracking**: Where did Alice go yesterday?
- **Meeting Disclosure**: How many times did Alice and Bob meet?

- R. Shokri, PhD Dissertation, EPFL 2013

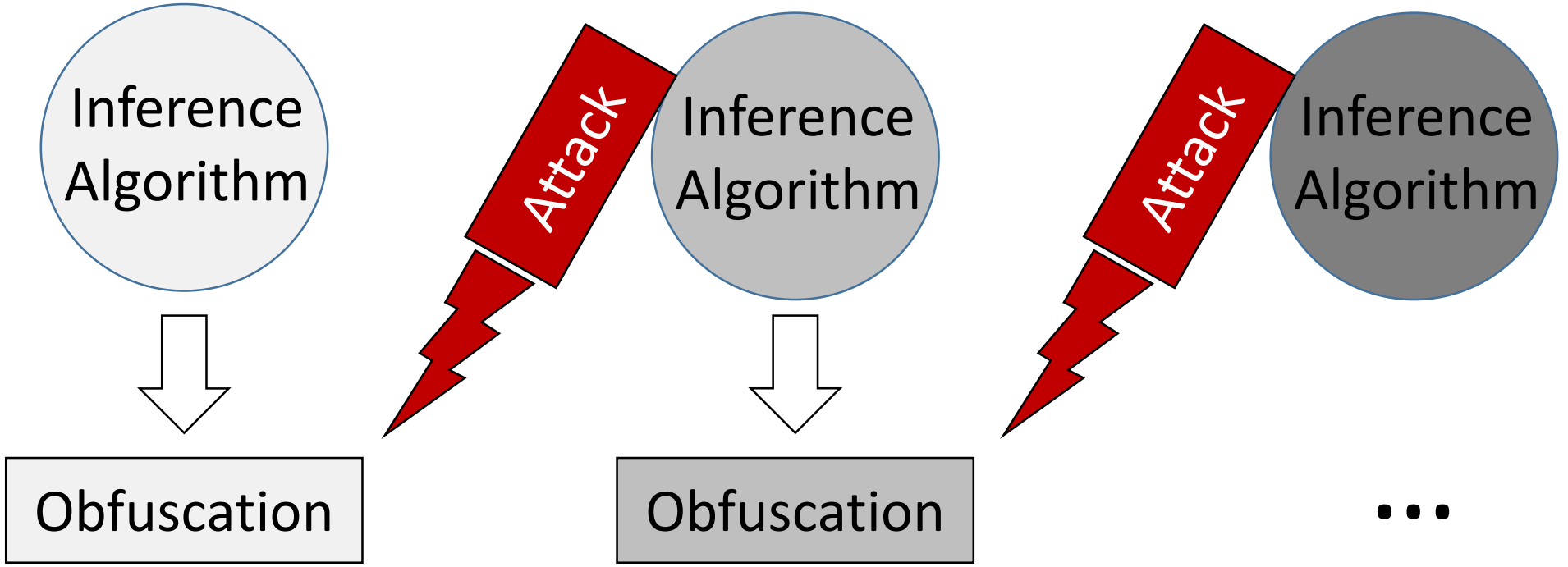
How to Optimally **Protect** Location Privacy using Obfuscation?



There is a tradeoff between **privacy** and **utility**

Solution: Decision Theory ?

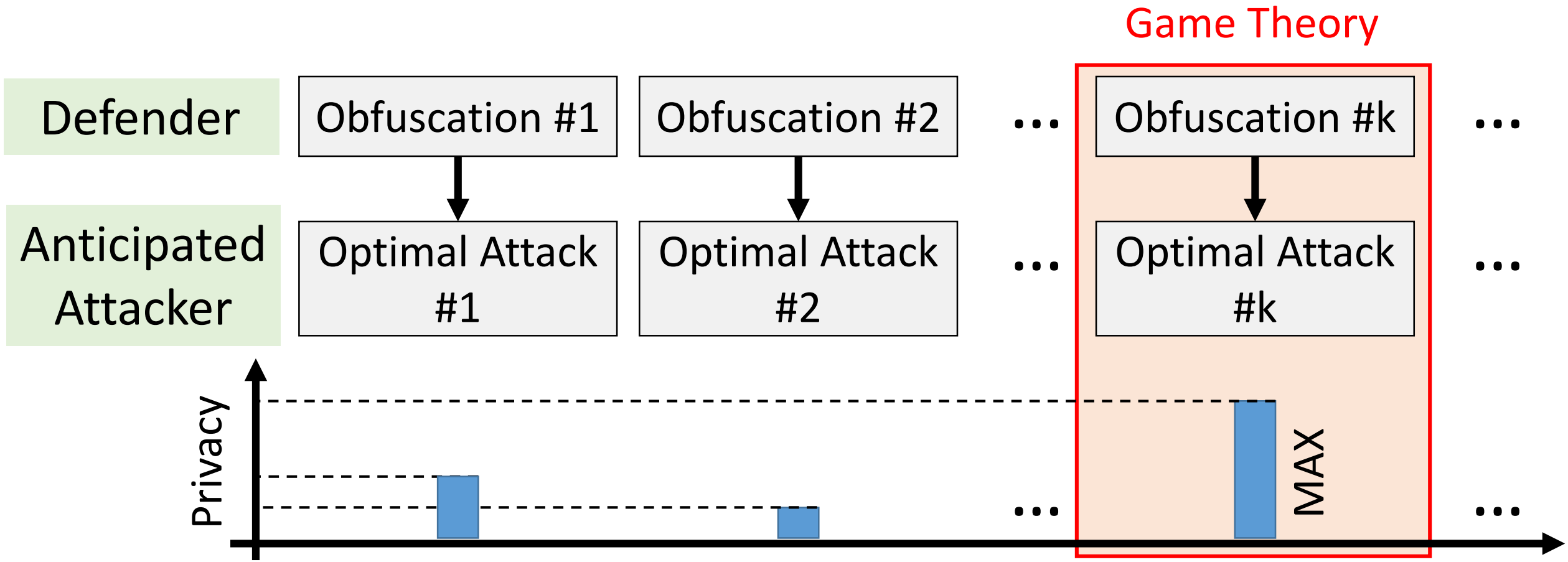
- Minimize privacy loss
  - Satisfy utility constraints



Privacy decision making must be **interactive**

Attacker Has the Upper Hand

Defender Must Anticipate the Inference Attack



- Solve **conflicting** optimizations: Defense and Attack

- R. Shokri, et al., "Protecting Location Privacy: Optimal Strategy against Localization Attacks," in ACM **CCS** 2012.

Conclusions

- Defense against surveillance
  - Practical protection mechanisms with theoretical foundations
  - Intelligent obfuscation methods, considering user behavior

- Computational privacy
  - Quantify privacy using statistical inference: measure adversary error
  - Protect privacy in a strategic decision making process: find the optimal balance between *privacy*, *utility*, and *computing* budgets