Investigate alternative architecture designs for providing personalized location privacy guarantee, while maintaining desirable quality of service requirements.

Exploits the intrinsic relationships between policy-based location privacy model and location-anonymity based privacy protection mechanisms.

Finding an optimal balance between location privacy and location service quality and introducing uncertainty on location-identity associations.

Scalable and attack resilient location cloaking algorithms.

Personalized Location Anonymization

Usage Model:
Privacy Requirements serve as constraints for location cloaking.
Location k-anonymity with variable k.
Location l-diversity with variable l.
Personalized maximum.
Spatial/Temporal Resolution.

Three Alternative Location Anonymization Models

Centralized corporative.
Decentralized non-corporative,
Device based.

Design Goals
Optimal Anonymization: cloaking as many messages as possible; minimizing dropped service requests due to location anonymization requirements given in the usage model.

Technical Challenges
How to balance location privacy and service quality?
How to provide personalized location privacy? variable k + variable l + personalized constraint box → maximum temporal and spatial location resolution.
What is the most scalable and yet effective architecture for supporting personalized location anonymity model?