Membership Inference

Yelp-health		FourSquare	
Batch Size	**Precision**	**Batch Size**	**Precision**
32	0.92	100	0.99
64	0.84	200	0.98
128	0.75	500	0.91
256	0.66	1,000	0.76
512	0.62	2,000	0.62

Two-Party Membership Inference
(Recall is 1.0)

Agenda

1. Membership Inference against Generative Models
2. Property Inference in Collaborative/Federated ML
3. Backdoor Attacks in Federated ML