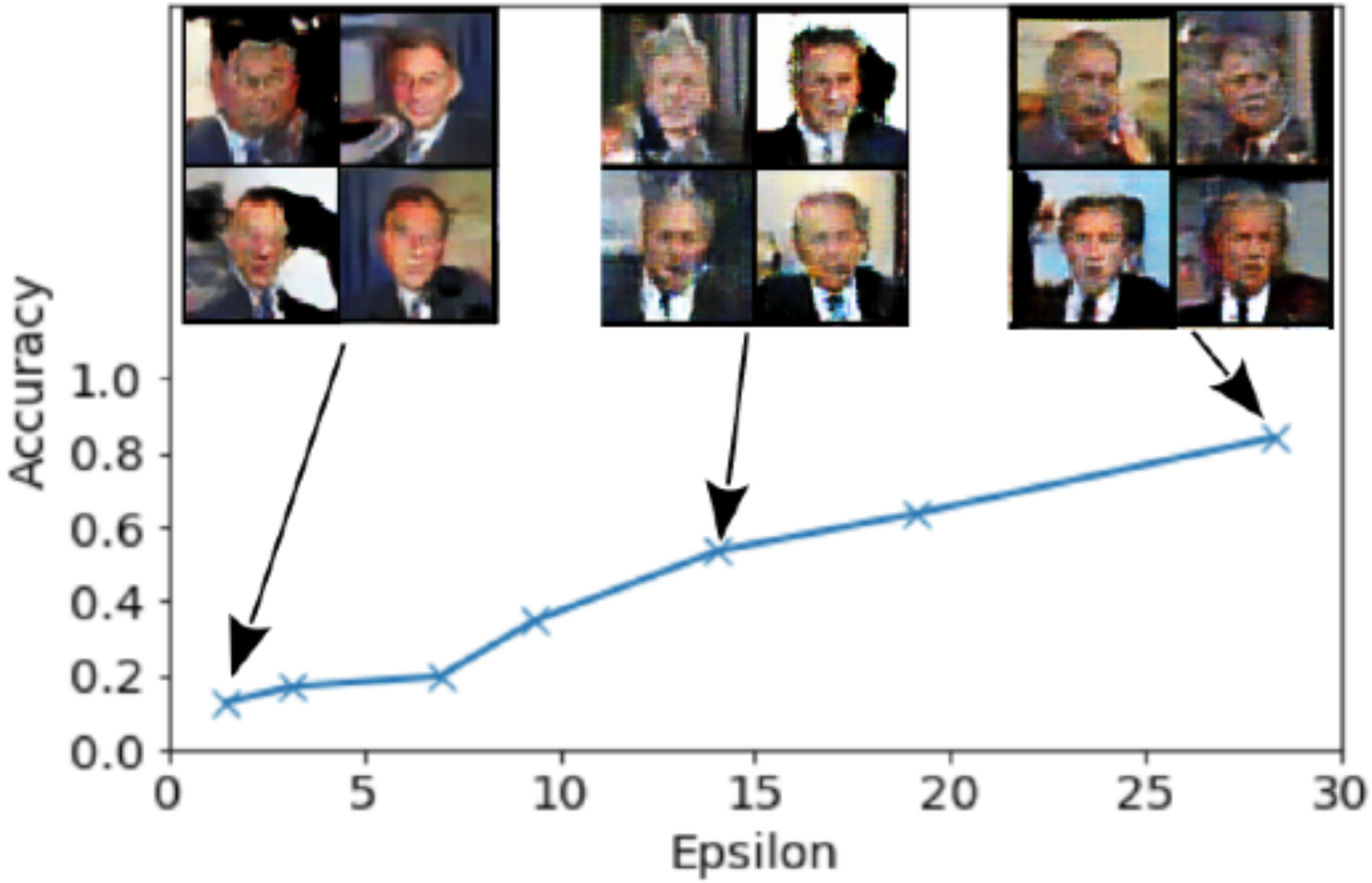
Defense? Differentially Private GAN?



White-box, LFW, top ten classes

Triastcyn et al. “Generating differentially private datasets using GANs.”

Agenda

1. Membership Inference against Generative Models

2. Property Inference in Collaborative/Federated ML

3. Backdoor Attacks in Federated ML