Reasoning about “privacy” in ML

Any useful machine learning model reveals something about the population from which the training data was sampled

Privacy leakage != Adv learns something new about training data


101
1101
01101
110101
110001
1001
Data Leakage

Reasoning about "privacy" in ML

Any useful machine learning model reveals something about the population from which the training data was sampled

Privacy leakage != Adv learns something new about training data

Reasoning about “privacy” in ML (2)