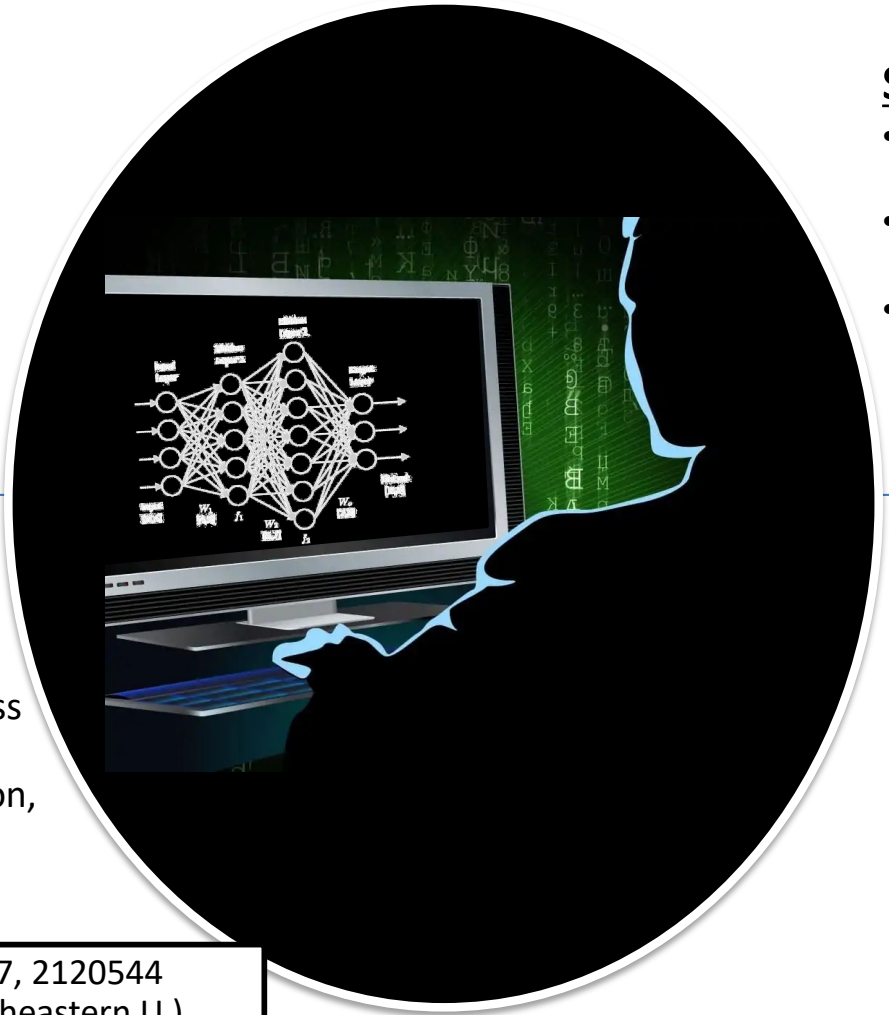
Foundations for the Next Generation of Private Learning Systems

Northeastern University | BOSTON UNIVERSITY | Carnegie Mellon | Columbia University

Challenge:

- Theoretical foundations of privacy-aware learning not well matched to structure of next-generation learning systems



Scientific Impact:

- Foundations for the next decade of privacy research
- New algorithms and auditing tools
- Explanations for recent phenomena: memorization, large models, and beyond

Solution:

- Theoretical foundations for privacy for learning systems
- Auditing tools for under-standing practical privacy loss
- Differentially private algorithms for personalization, transfer learning, continual learning

Broader Impact and Broader Participation:

- Privacy continues to be a central challenge for ethical data-driven systems
- Expanded toolkit for deployments in
  - Industry (Google, Apple, …)
  - Government (Census, IRS, …)
- New course materials, textbook, K-12 outreach

Award # 2120603, 2120611, 2120667, 2120544
Alina Oprea, Jonathan Ullman (Northeastern U.)
Steven Wu (Carnegie Mellon U.)
Roxana Geambasu (Columbia U.)
Adam Smith (Boston University)