PROJECT SUMMARY

Overview:

Interactive online decision making, one key learning paradigm of machine learning (ML), has thoroughly permeated into our everyday life through a variety of applications ranging from personalized recommendation systems (e.g., advertisements, mobile healthcare) to real-world robots and autonomous driving. These applications are particularly data-hungry as they rely heavily on users' feedback and personal information to improve the their recommendations or control policies on the fly. However, the use of personal data in these applications poses significant risks for privacy. In fact, several real-world empirical studies have reported privacy breaches in nowadays recommendation and autonomous driving systems. Therefore, there exists a fundamental conflict between users' privacy protection and the utility of data-driven online learning applications, i.e., privacy-utility trade-off. The goal of this project is to take the first step towards a comprehensive understanding of privacy-utility trade-offs in the paradigm of online decision making.

Keywords: Differential privacy; Online decision making; Bandit learning; Reinforcement learning; Regret minimization; Privacy auditing; Real-world robots;

Intellectual Merit:

The overarching theme of this CAREER research program is to to provide theoretical and algorithmic foundations of privacy-preserving online decision making. To this end, we leverage the mathematical tools of differential privacy (DP) and regret minimization to formally characterize privacy and utility, respectively. We aim to provide a unified view of DP online learning under different learning models (e.g., different bandits and reinforcement learning models), different learning architectures (single learner and various federated learning settings) and different DP trust models (e.g., central, local and distributed DP models), bridging the existing gap in privacy protection for online learning and advancing the state-of-the-art.

We start with three complementary research thrusts that are not only closely inter-connected with each other, but draw novel connections with DP supervise learning frameworks such as DP empirical risk minimization (DP-ERM), DP stochastic convex optimization (DP-SCO). In Thrust 1, we study the core problem of how to achieve a refined privacy-utility trade-off via new DP models that are beyond the classic central and local ones. In Thrust 2, we move to the federated online learning setting where multiple local agents work in concert to realize a collaborative learning with sparse communication while guaranteeing privacy protection to each local user. In Thrust 3, we step back to explore the possibility of developing a plug and play algorithmic framework for private online learning that automatically adapts to the underlying function classes (e.g., linear functions, generalized linear functions, kernels and neural networks).

We will empirically evaluate both privacy loss and utility performance of the proposed algorithms in all three thrusts. We propose a novel privacy auditing scheme by designing various adversaries to measure the actual privacy loss. We will also leverage open-sourced platforms and our access to real-world robots and self-driving cars to conduct large-scale empirical studies of the utility in the real-world scenarios.

Broader Impacts:

From a societal impact perspective, a privacy-preserving online decision making enabled by this project allows people to enjoy the benefits of various personalized services while without worrying too much about the privacy leakage, especially the minorities who were often more vulnerable under privacy attacks due to their unique features. From an economic and industry impact perspective, a personalized service accompanied by the feature of privacy protection and efficient utility guarantees allows the service providers to attract more users and hence increase the profit. Moreover, the outcomes of this project enjoy potential commercial interactions with companies ranging from autonomous vehicles to recommendation systems, hence impacting the society at-large. From an education perspective, this project enables to develop curriculum that will be broadly shared, as well as train undergraduate and graduate students. Special attention will be devoted to recruiting a diverse group of students and provide them opportunities for career development. Finally, we will reach out to middle and high school students by organizing workshops on privacy-preserving online decision making based on demos of our real-world robots and self-driving cars, partnered with excellent outreach programs at Wayne State University.