CS 208 - Applied Privacy for Data Science
Project Proposal

Jason Huang
Spring 2019 - Harvard University

1. **Practical Differential Privacy for Distributed Users**: This is effectively a study and in-depth investigation into what has become a common application of differential privacy: collecting data in a locally manner from a large population of users over time. These are particularly evident with commercial deployments such as within Apple's iOS and Google's RAPPOR system. These and other deployments will likely be examined in-detail and their shortcomings detailed. Ideally, some formal evaluation of their shortfalls can be calculated or, optimistically, possibly even running some sort of attack in a controlled ethical manner to demonstrate these shortfalls. Then, if ideas arise, proposals for improvement will be raised. In particular, this project would draw from literature revolving around these deployments, as well as the theoretical foundations of local differential privacy and differential privacy under continual observation.

   To summarize, studying deployments specifically Apple's iOS and Google's RAPPOR, along with studying literature on attacks, local differential privacy and differential privacy under continual observation.

   Some concerns that may arise with this are particularly: while there is lots of literature behind these deployments, how would any practical evaluation of these systems work; of course, taking into account controlled ethical concerns of working with a live system (likely requiring their permission). A somewhat more significant concern for me; is there any particular area I can investigate to bring new ideas and suggestion to the literature rather than just reiterate what already exists?

   Some citations (detailed formal annotated bibliography can be provided upon request):

   - Apple's system: https://machinelearning.apple.com/docs/learning-with-privacy-at-scale/appledifferentialprivacysystem.pdf
   - Google's RAPPOR: https://static.googleusercontent.com/media/research.google.com/en//pubs
   - Local Differential Privacy Under Evolving Data: https://arxiv.org/abs/1802.07128
   - Differential Privacy Under Continual Observation: https://www.cs.toronto.edu/ toni/Papers/dp observation.pdf