To: economist working group

Questions for discussion on October 10, 2024

We would like to discuss plans for the validation server rollout and development at our next meeting. Here are a few questions that we could use help with. Several follow up on the discussion we had at the last meeting.

1. What kinds of analysis would be most useful to be able to perform using the validation server

Background: Urban Institute has a prototype validation server that can produce privacy-protected statistics of certain types including OLS and logit regression and univariate statistics. Our ultimate goal is to be able to handle complex statistical queries, but the validation server team would like to know what kinds of analyses would be most useful to prioritize as steps towards this goal.

1. We have discussed the privacy budget which would limit the total number of statistical analyses or other queries that could be run before the researcher would have to stop. The privacy budget is well defined in the context of differential privacy, but in methods that are not formally private, the concept is kind of *ad hoc*. Is the concept of a privacy budget useful outside of a formally private framework? If so, how should it be implemented? If not, how should an automated validation server guard against abuse (e.g., running equivalent statistical queries a large number of times to eliminate the effects of noise infusion).
2. We are using methods based on the maximum-observed sensitivity algorithm developed by Raj Chetty and John Friedman to estimate the amount of noise to add to estimates. This method may not be computationally feasible for more complex estimation methods, especially if applied to large datasets. We are thinking of simpler noise infusion methods. One option would use computational derivatives to estimate the noise. Rob McClelland discussed this method based on Broderick, et al. (attached), in a previous meeting. Another would estimate MOS based on samples of the dataset. Max Ghenis, who we’ve invited to join our group, suggested using estimates derived from both the synthetic data and the confidential data to implicitly inject noise. The question is: how can we estimate the efficacy of those methods—both in terms of utility and privacy.

Background: The advantage of differential privacy is that it does not assume a particular kind of threat or anything particular about the data possessed by a potential intruder. But formally DP methods have only been derivable for a limited set of estimators. In addition, the concept of global privacy often requires a large—probably excessive—amount of noise unless ε is set quite large. The MOS method is not globally private but can still require a large amount of noise. Suppose we added much less noise. Could we develop an empirical threat model that would encompass the range of plausible threats to the data that we could use to assess the privacy protection that would arise from these *ad hoc* noise infusion methods. (I know this is kind of poorly formulated but hope it’s a useful starting point for discussion.)