Abstract: We propose a general optimization-based framework for computing differentially private M-estimators and a new method for the construction of differentially private confidence regions. Firstly, we show that robust statistics can be used in conjunction with noisy gradient descent and noisy Newton methods in order to obtain optimal private estimators with global linear or quadratic convergence, respectively. We establish global convergence guarantees, under both local strong convexity and self-concordance, showing that our private estimators converge with high probability to a neighborhood of the non-private M-estimators. The radius of this neighborhood is nearly optimal in the sense it corresponds to the statistical minimax cost of differential privacy up to a logarithmic term. Secondly, we tackle the problem of parametric inference by constructing differentially private estimators of the asymptotic variance of our private M-estimators. This naturally leads to the use of approximate pivotal statistics for the construction of confidence regions and hypothesis testing. We demonstrate the effectiveness of a bias correction that leads to enhanced small-sample empirical performance in simulations.

This is joint work with Casey Bradshaw and Po-Ling Loh

Bio: Marco Avella Medina is an assistant professor in the Department of Statistics at Columbia University. His research interests include robust statistics, high-dimensional statistics and differential privacy. Before joining Columbia, he was a postdoctoral fellow at MIT, where he was affiliated with the Sloan School of Management and the Statistics and Data Science Center. He holds a B.A. degree in Economics, a M.Sc. degree in Statistics and a Ph.D. in Statistics, all from the University of Geneva, Switzerland.