Title: Estimation and Privacy

Speaker: Dr. Flavio Calmon, IBM T.J. Watson Research Center and Harvard University

Date: Thursday, April 21, 2016 11am

Abstract:

Widespread collection of data has led to new and challenging privacy and security risks. There is a need to engineer mechanisms that allow users to selectively disclose their data to a third party in order to achieve a utility goal (e.g. receive high quality product recommendations), while restricting the release of private information (e.g. not revealing a given medical condition). In this talk, we use tools from information theory, statistics and estimation theory to characterize the fundamental limits of estimation when only partial statistics of the data are known. We then apply the insight gained by characterizing these limits to quantify the fundamental privacy-utility tradeoff and to design privacy-assuring mechanisms. In addition, we introduce security metrics and associated results based on the spectrum of the conditional expectation operator, called the principal inertia components. The principal inertia components allow a fine-grained decomposition of the dependence between a hidden and an observed variable which, in turn, is useful for deriving fundamental bounds for estimation problems, and for measuring information leakage in secure communication models.

Bio:

Flavio du Pin Calmon is a post-doctoral researcher at the IBM T.J. Watson Research Center and an associate in Electrical Engineering at Harvard. His research interests include information theory, data analytics, statistics, estimation theory, security and privacy. Before coming to IBM, he received a Ph.D. in Electrical Engineering and Computer Science at MIT, an M.Sc. in Electrical Engineering from the Universidade Estadual de Campinas, Brazil, and a B.Sc. in Communications Engineering from the Universidade de Brasilia, Brazil