Differential privacy in practice: benefits and challenges

Gerome Miklau, Tumult Labs

Abstract:
Differential privacy is a model of privacy protection currently being adopted by both commercial enterprises and government institutions. The goal of this talk is to review the benefits differential privacy can offer to custodians of sensitive data, as well as key challenges to its adoption and practical deployment. This talk will reflect my perspective as an academic researcher into differential privacy as well as my experience as a founder of Tumult Labs, a startup that is commercializing differential privacy and helping to deploy it at a range of institutions.

Using differential privacy, data custodians can share data in new ways while confidently managing privacy risk. They can enjoy the benefits of strong resistance to potential privacy attacks and compliance with a wide range of regulation. But adoption of differential privacy has, to date, most often succeeded in institutions with very sophisticated technical capabilities. Using existing tools to build differentially private data release systems remains challenging. In addition, setting privacy parameters, assessing tradeoffs between acceptable privacy loss and accuracy, and communicating error to stakeholders, often require the assistance of experts. I will speculate on which of the challenges can be addressed through automation or better interfaces, and which require research advances.

Bio (Gerome Miklau)
Gerome Miklau is a professor in the Manning College of Information and Computer Sciences at the University of Massachusetts Amherst. His research focuses on private, secure, and equitable data management. He designs algorithms to accurately learn from data without disclosing sensitive facts about individuals, primarily in the model of differential privacy. In 2019 he co-founded Tumult Labs, a start-up focused on commercializing privacy technology. Prior to that, he consulted for the U.S. Census Bureau on algorithms that have been deployed as part of the 2020 decennial census. Professor Miklau received the ACM PODS Alberto O. Mendelzon Test-of-Time Award in 2020 and 2012, the Best Paper Award at the International Conference of Database Theory in 2013, and an NSF CAREER Award in 2007. He received his Ph.D. in Computer Science from the University of Washington in 2005.