## PPAI-20 Technical Program

**8:45 - 9:00**: Poster Setup and Opening Statement

**9:00 - 9:45**: [Invited Talk](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/index.html#invited1): Catuscia Palamidessi

**9:45 - 10:30**: Session I

Session Chair: TBA  
Gilie Gefen, Omer Ben-Porat, Moshe Tennenholtz and Elad Yom-Tov.  
[*Assessing the Value of Internet Data for Medical Applications*](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/papers/paper_8.pdf)*.*

Reza Shokri, Martin Strobel and Yair Zick.  
[*Exploiting Transparency Measures for Membership Inference: a Cautionary Tale*](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/papers/paper_17.pdf)*.*

Shubhankar Mohapatra, Xi He, Gautam Kamath and Om Thakkar.  
[*Diffindo! Differentially Private Learning with Noisy Labels*](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/papers/paper_23.pdf)*.*

**10:30 - 11:00**: Break and Poster Session

**11:00 - 11:45**: [Invited Talk](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/index.html#invited2): Boi Faltings

**11:45 - 12:30**: Poster Session

**12:30 - 13:50**: Lunch (not sponsored)

**13:50 - 14:45**: Panel Discussion Topic: “Grand Challenges in Privacy in 2020: What are they and what are we missing?"

Members TBA

**14:45 - 15:30**: [Invited Talk](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/index.html#invited3): Aleksandar Nikolov

**15:30 - 16:00**: Break and Poster Session

**16:00 - 16:45**: Poster Session

**16:45 - 17:30**: Session II

Session Chair: TBA

Kai Wen Wang, Travis Dick and Maria-Florina Balcan.  
[*Scalable and provably accurate algorithms for differentially private distributed decision tree learning*](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/papers/paper_12.pdf)*.*

Chaitali Ashok Choudhary, Martine De Cock, Rafael Dowsley, Anderson Nascimento and Davis Railsback.  
[*Secure Training of Extra Trees Classifiers over Continuous Data*](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/papers/paper_24.pdf)*.*

Dominik Fay, Jens Sjölund and Tobias J. Oechtering.  
[*Private Learning for High-Dimensional Targets with PATE*](https://www2.isye.gatech.edu/~fferdinando3/cfp/PPAI20/papers/paper_29.pdf)*.*

**Invited Speakers**  
[**Boi Faltings**](https://people.epfl.ch/boi.faltings?lang=en) **(EPFL)**

*Privacy-Preserving Constraint Optimization*Artificial Intelligence can play an important role in modern society as a mediator between different parties, such as auctions and coordination mechanisms. However, the preferences and constraints involved in such mediation are private information and must be protected from leakage both to the mediator and to the other parties. I present different solutions to this problem based on homomorphic encryption and multiparty computation, and discuss open issues for further research. 

[**Catuscia Palamidessi**](http://www.lix.polytechnique.fr/Labo/Catuscia.Palamidessi/) **(INRIA)**TBA

[**Aleksandar Nikolov**](http://www.cs.toronto.edu/~anikolov/)**(University of Toronto)**

*The Power of Factorization Mechanisms for Answering Counting Queries*Many tasks in private data analysis can be reduced to answering a collection of counting queries, i.e. queries that ask what fraction of the dataset satisfies a given property. Counting queries, for example, capture contingency tables and CDFs, and can be used to implement learning algorithms in the Statistical Query model. A basic method to answer counting queries with differential privacy is to add IID Laplace or Gaussian noise to the query answers. Often, however, one can get much better error guarantees by instead answering a different set of “strategy queries” with IID noise, and then reconstructing answers to the original queries. Optimal strategy queries can be usually computed efficiently using convex optimization. The resulting factorization mechanisms give optimal error vs privacy trade-offs in various models of differential privacy and parameter regimes. In this talk, I will give a flavor of factorization mechanisms, and what we can prove about them.