

NIST and Differential Privacy

How NIST uses crowdsourcing to advance the field of differential privacy

This challenge had a significant impact on the privacy community. The problem we put forth to the crowd was previously considered potentially unsolvable by many, even by some of the challenge participants, and the results of crowdsourcing proved otherwise.

Dr. Christine Task
Senior Computer Scientist, Knexus Research Corporation
NIST Contractor, Project Technical Lead

The National Institute for Standards and Technology's Public Safety Communications Research Division (NIST PSCR) is successfully tackling some of the thorniest issues surrounding privacy with the help of crowdsourcing. As a result of the challenges run on the HeroX platform, they've achieved these great results:

- The differential privacy community has expanded beyond subject matter experts, recruiting new data scientists.
- Innovators voluntarily open-sourced their code for use by the research community.
- Rapid and unprecedented progress was made in developing differential privacy algorithms due to the head-to-head competitive nature of the challenge.
- The Privacy Community is exploring other ways to use challenges as a means to encourage risk-taking and motivate deeply focused progress on a very challenging real-world problem.

CrowdPiper

powered by HeroX

In today's digital world, nearly every action we take generates data - whether you are browsing the internet, purchasing an item, or driving by a traffic camera. In the Public Safety Sector, analysis of this data can improve the protection of people and communities. Outside the Public Safety Sector, these datasets can help businesses understand consumer spending behavior, show municipal traffic patterns, and reveal emerging economic trends. However, privacy concerns currently limit how and when these datasets can be analyzed. Differential privacy techniques provably prevent the disclosure of personally identifiable information while preserving the utility of the dataset for analysis.

Current data anonymization algorithms are inadequate. In some cases, data can still be traced back to an individual. In other cases, the algorithm changes the data so much that it isn't useful anymore because it no longer allows the same conclusions to be drawn that would have been from the original, non-anonymized data.

To accelerate the pace at which progress is being made on this problem, NIST PSCR collaborated with HeroX, NASA Tournament Labs, and Topcoder to design and implement a crowdsourcing challenge to advance the field of differential privacy. This challenge was the first of its kind to benchmark the effectiveness of different solutions against each other. The multi-phased challenge broke the problem down into smaller, more digestible pieces and allowed for iterations between stages to maximize the project's effectiveness and success. This approach simultaneously made the problem easier to address and provided more opportunities for head to head competition, which has proven key to maintaining forward momentum. Additionally, outreach efforts for this challenge brought in innovators from outside the privacy community. These new participants help raise the profile of the problem while bringing in more diverse perspectives.

The results of this challenge surpassed all expectations of NIST PSCR, and they intend to share the challenge results in upcoming publications. The source code from several of the winning teams was open-sourced, and it is publicly posted [here](#). NIST made significant progress in this field, but there is still further research needed. NIST is considering future challenges to continue pushing forward with the differential privacy efforts.

This case study shows how even the toughest, most intractable problems can be addressed with crowdsourcing. For NIST, making the problem less theoretical and more concrete by staging regular competitions helped increase the pace at which advancements are being made.

To learn more and to see examples of other types of problems that can be crowdsourced, visit our [Resources page](#). If you have specific questions and would like to speak with an expert — email us at possibilities@herox.com.