Usable and Secure Data Analysis
Mayank Varia, Boston University, varia@bu.edu

Problem
aggregate sensitive salary data, calculate pay equity

Usability
increases confidence, participation, and security

Methodology & Interface

Design features:

Ease of use
Auditable
Comprehension
Idempotent
Feedback

Outcomes:

Confidence
Participation
User error
Security

Contributors only learn what the trusted party tells them.
The aggregator never learns anything. Neither
does any hacker attacking it.
Trusted party only learns analytics that were authorized
by contributors.

Methodology & Interface

Contributors only learn what the trusted party tells them.
The aggregator never learns anything. Neither
does any hacker attacking it.
Trusted party only learns analytics that were authorized
by contributors.

Reaction

The congresswoman, who had signed onto a bill
dressing income disparity between men and women,
was impressed by the relevance he outlined. "It's
linking it back for the members of Congress," Clark said.
"Nobody would think, oh, the
Paycheck Fairness Act, how is
that tied into NSF funding?"

BWWC co-chair Evelyn Murphy on secure multi-party computation:
"It’s used in computer science applications, but it
has never been used for public good. Here, we’re
beginning to show how to use this sophisticated
computer science research for public programs."

Extensions

1. Scale to big data
2. Integrate with legacy code

Setup
Runtime

Insecure baseline 16.2 min
Our system 17.5 min
Secure baseline > 120 min

More info

Collaborators

• Azer Bestavros
• Frederick Jansen
• Andrei Lapets
• Malte Schwarzkopf
• Nikolaj Volgushev

References

1. User-centric Distributed Solutions for Private-
    preserving Analytics, Cores of the ACM, 2017
2. Secure Multi-Party Computation for Analytics
    Deployed as a Lightweight Web Application, SecDev 2016
4. Programming Support for an Integrated Multi-
    Party Computation and MapReduce
5. Scatter: Programming with Multi-party
    Computation & MapReduce. BU CS Tech Report