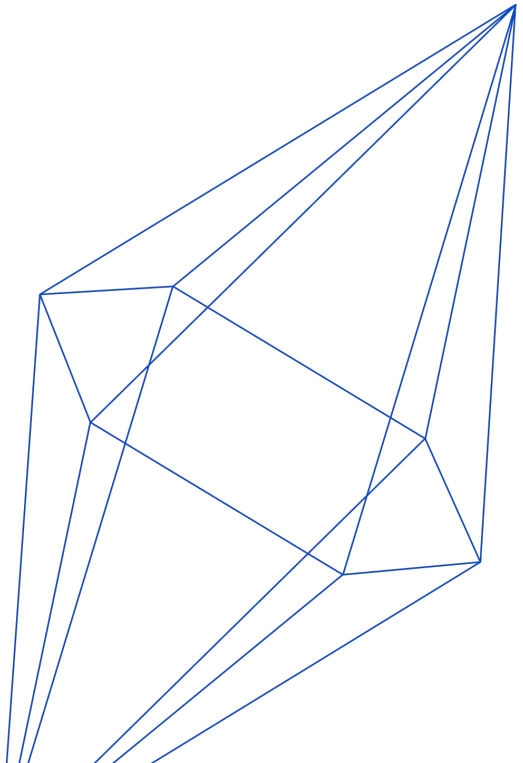
# PHSafe: The Disclosure Avoidance Algorithm for the Supplemental Demographic and Housing Characteristics File

William Sexton, Ashwin Machanavajjhala, David Pujol



William Sexton• Sr. Scientist • william.sexton@tmlt.io

FCSM Conference, October 2024

# Goals

- What is PHSafe?

- Development workflow for deploying DP
  - How does PHSafe work?
  - When does PHSafe work well?
  - Why does PHSafe work?

# What is PHSafe?

## Disclosure Avoidance and the Supplemental Demographic and Housing Characteristics File (S-DHC): How PHSafe Works

*2020 Census Briefs*

By the Population Reference Bureau and
the U.S. Census Bureau's 2020 Census Data Products and Dissemination Team

https://www2.census.gov/library/publications/decennial/2020/census-briefs/c2020br-12.pdf

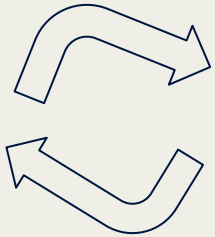
## Tumult's Methodology for Deploying Differential Privacy

### Design

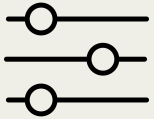
What are the tabular summaries to release?

What are the privacy and accuracy requirements?

What is the algorithmic strategy?



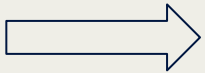
### Tune



What are the tunable parameters that affect privacy and accuracy?

Can we quantify the relationship between privacy and accuracy?

How do we choose the right parameters?



### Deploy

Is the algorithm implemented correctly? Is it provably private?

How do we communicate the privacy accuracy tradeoffs inherent in the implementation?

# Outline

- **Designing PHSafe**
- Tuning PHSafe
- Deploying PHSafe

# Design: What are the tabular summaries?

**PH1 Num**
Average Household Size By Age

**PH1 Denom**
Average Household Size By Age

**PH2**
Household Type for the Population in Households

**PH3**
Household Type by Relationship for the Population Under 18 Years

**PH4**
Population in Families by Age

**PH5 Num**
Average Family Size by Age

**PH5 Denom**
Average Family Size by Age

**PH6**
Family Type and Age for Own Children Under 18 Years

**PH7**
Total Population in Occupied Housing Units by Tenure

**PH8 Num**
Average Household Size of Occupied Housing Units by Tenure

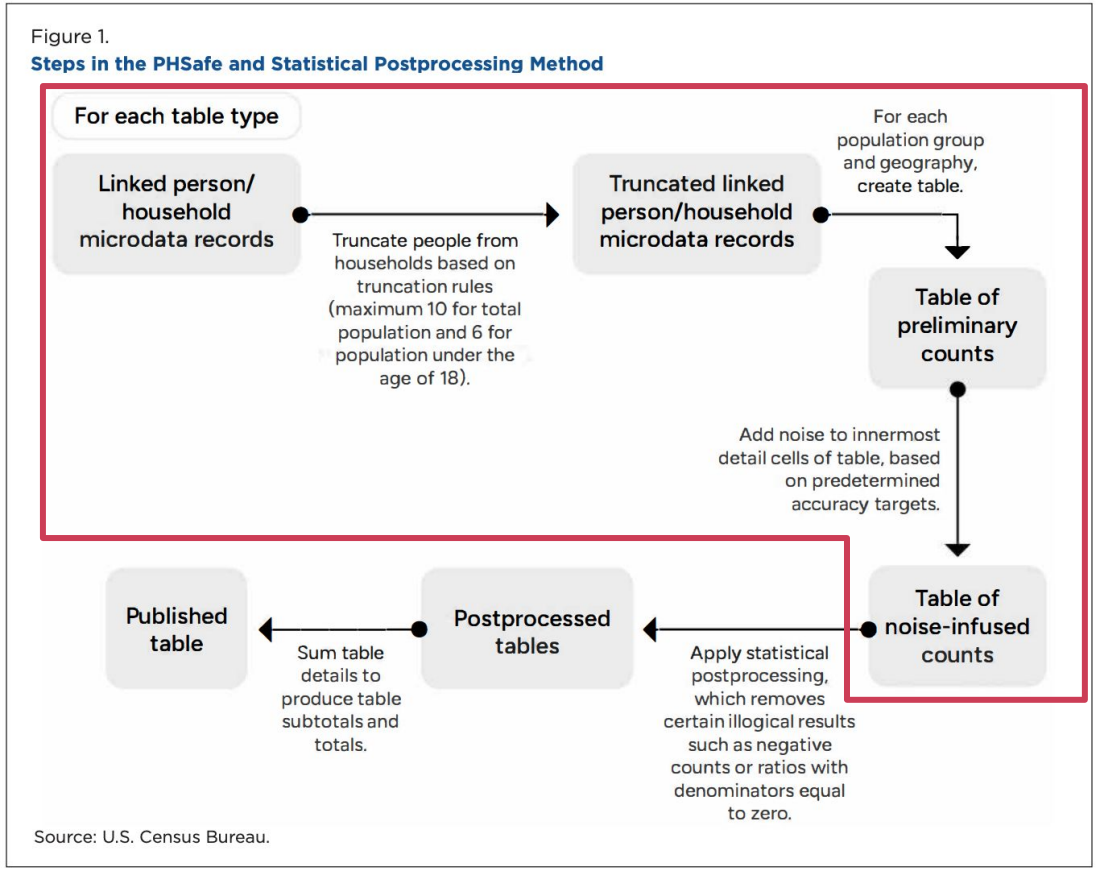
**PH8 Denom**
Average Household Size of Occupied Housing Units by Tenure

# Design: What are the privacy and accuracy requirements?

- **Privacy:** PHSafe must satisfy zero-concentrated differential privacy (zCDP).

- **Accuracy:** PHSafe's noise infusion must be tunable to achieve desired 90% margins of error (MOE).

# Design: What is the algorithmic strategy?



# Joined Data

| PersonID | HouseholdID | Relationship |
|---|---|---|
| Person 1 | Household A | Householder |
| Person 2 | Household A | Spouse |
| Person 3 | Household A | Biological Child |
| Person 4 | Household A | Biological Child |
| Person 5 | Household A | Biological Child |
| Person 1 | Household B | Householder |
| Person 2 | Household B | Unmarried Partner |

| HouseholdID | Household Size | Household Type |
|---|---|---|
| Household A | 5 | Married Couple Family |
| Household B | 2 | Non Family |
| Household C | 4 | Single Parent Family |

# Disclosure risks with Joined Data

| PersonID | HouseholdID | Relationship |
|---|---|---|
| Person 1 | Household A | Householder |
| Person 3 | Household B | Biological Child |
| Person 3 | Household A | Biological Child |
| Person 4 | Household A | Biological Child |
| Person 5 | Household A | Biological Child |
| Person 1 | Household B | Householder |
| Person 2 | Household B | Unmarried Partner |

| HouseholdID | Household Size | Household Type |
|---|---|---|
| Household A | 4 | Single Parent Family |
| Household B | 3 | Cohabiting Couple Family |
| Household C | 4 | Single Parent Family |

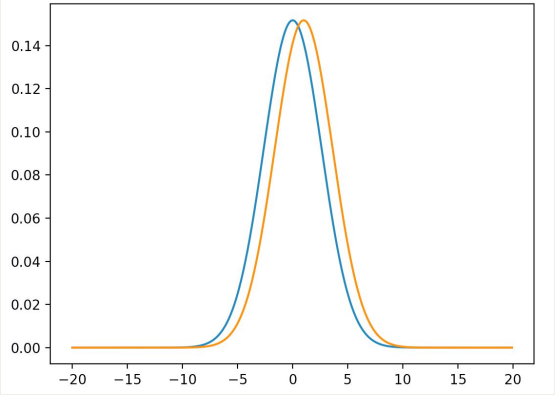
# Disclosure risks with Joined Data

| PersonID | HouseholdID | Relationship |
|---|---|---|
| Person 1 | Household A | Householder |
| Person 3 | Household B | Biological Child |
| Person 3 | Household A | Biological Child |
| Person 4 | Household A | Biological Child |
| Person 5 | Household A | Biological Child |
| Person 1 | Household B | Householder |
| Person 2 | Household B | Unmarried Partner |

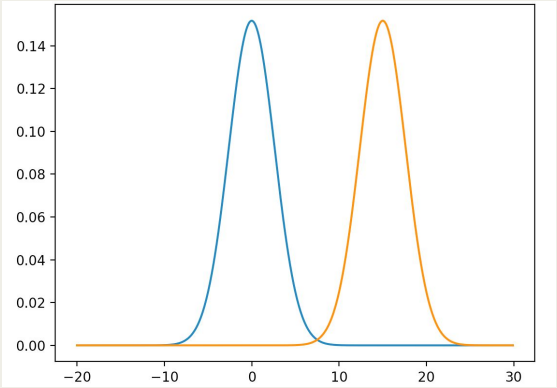
| HouseholdID | Household Size | Household Type |
|---|---|---|
| Household A | 4 | Single Parent Family |
| Household B | 3 | Cohabiting Couple Family |
| Household C | 4 | Single Parent Family |

# Disclosure risks with Joined Data

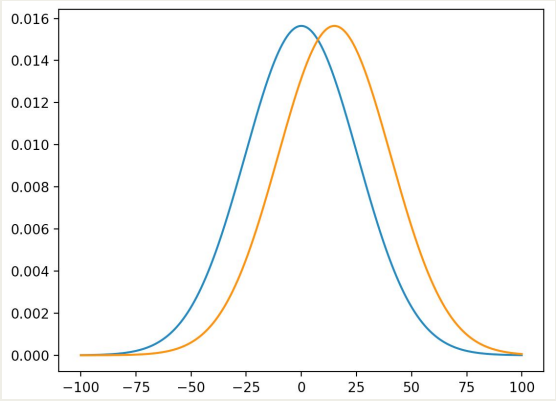
Low influence scenario.
Max household size = 1
MOE = 5, low disclosure risk




High influence scenario.
Max household size = 15
MOE = 5, high disclosure risk




High influence scenario.
Max household size = 15
MOE = 50, low disclosure risk



# Truncation

- Limits the number of people in households to not exceed a given threshold.
- Ignores out of universe
- Randomly selects in-universe records for removal as needed.

Table 2.

**Illustration of Truncation for Household Maximum of Six People Under the Age of 18**

| Initial household | Person number in the enumerated household | Age | In universe? | Action | Person number in the truncated household |
|---|---|---|---|---|---|
| Household A | 1 | 51 | Not in universe. | Exclude from universe. | Not in universe. |
| Household A | 2 | 49 | Not in universe. | Exclude from universe. | Not in universe. |
| Household A | 3 | 17 | In universe. | No change. | 1 |
| Household B | 1 | 63 | Not in universe. | Exclude from universe. | Not in universe. |
| Household B | 2 | 40 | Not in universe. | Exclude from universe. | Not in universe. |
| Household B | 3 | 22 | Not in universe. | Exclude from universe. | Not in universe. |
| Household B | 4 | 2 | In universe. | No change. | 1 |
| Household B | 5 | 5 | In universe. | No change. | 2 |
| Household B | 6 | 1 | In universe. | No change. | 3 |
| Household B | 7 | 2 | In universe. | Selected at random for removal. | Not included. |
| Household B | 8 | 5 | In universe. | Selected at random for removal. | Not included. |
| Household B | 9 | 6 | In universe. | No change. | 4 |
| Household B | 10 | 6 | In universe. | Selected at random for removal. | Not included. |
| Household B | 11 | 9 | In universe. | No change. | 5 |
| Household B | 12 | 17 | In universe. | No change. | 6 |
| Household C | 1 | 26 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 2 | 22 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 3 | 24 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 4 | 23 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 5 | 21 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 6 | 21 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 7 | 19 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 8 | 19 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 9 | 19 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 10 | 18 | Not in universe. | Exclude from universe. | Not in universe. |
| Household C | 11 | 17 | In universe. | No change. | 1 |
| Household C | 12 | 17 | In universe. | No change. | 2 |

Source: U.S. Census Bureau.

# Truncation

**PH1 Num**
Average Household Size By Age

$\tau = 10$

**PH2**
Household Type for the Population in Households

$\tau = 10$

**PH3**
Household Type by Relationship for the Population Under 18 Years

$\tau = 6$

**PH4**
Population in Families by Age

$\tau = 10$

**PH5 Num**
Average Family Size by Age

**PH6**
Family Type and Age for Own Children Under 18 Years

$\tau = 6$

**PH7**
Total Population in Occupied Housing Units by Tenure

$\tau = 10$

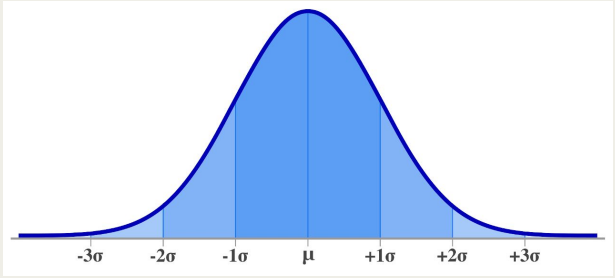
**PH8 Num**
Average Household Size of Occupied Housing Units by Tenure

Not directly computed by PHSafe

Directly computed by PHSafe

# Noise Infusion

**PH2: Household Type for the Population in Households**
*Universe: Population in households.*
Total:
- In married couple household:
  - Opposite-sex married couple
  - Same-sex married couple
- In cohabiting couple family:
  - Opposite-sex cohabiting couple
  - Same-sex cohabiting couple
- Male householder, no spouse or partner present:
  - Living alone
  - Living with others
- Female householder, no spouse or partner present:
  - Living alone
  - Living with others



# Noise infusion

The discrete Gaussian distribution $\mathcal{N}_{\mathbb{Z}}(\sigma^2)$ centered at 0 is

$$\forall x \in \mathbb{Z}, \quad \Pr[X = x] = \frac{e^{-x^2/2\sigma^2}}{\sum_{y \in \mathbb{Z}} e^{-y^2/2\sigma^2}}.$$

$\sigma^2 = (2\tau+2)^2 / \varrho$

| PH1_num | Total | Iteration H,I | Iterations A-G |
|---|---|---|---|
| Nation | | ?? | |
| State | | | |

| PH2 | Total |
|---|---|
| Nation | ?? |
| State | |

# Outline

- Designing PHSafe
- **Tuning PHSafe**
- Deploying PHSafe

# Tuning: What are the tunable parameters that affect privacy and accuracy?

- Privacy-loss budget
- Truncation threshold
- 90% MOE
- Geography levels
- Race Iterations

# Tune: What is the relationship between privacy and accuracy?

$$\sigma^2 = (2\tau+2)^2 / \varrho$$

90% MOE = $1.645\sigma$

$$\varrho = 1.645^2(2\tau+2)^2 / \text{MOE}^2$$

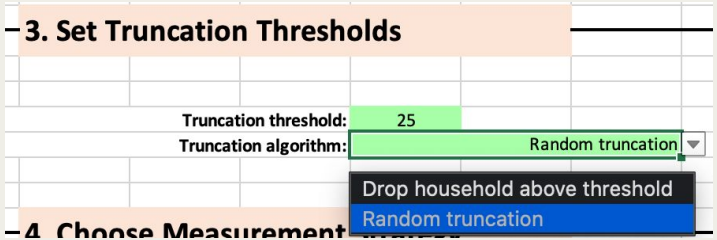
$\tau$=10, MOE=200 $\Rightarrow$ $\varrho$ = 0 .0327

# Tune: How do we choose the right parameters?

## 1. Specify Privacy Loss Budget Parameters

| | | Geography Enabled | Total Epsilon |
|---|---|---|---|
| Geography | USA | TRUE | 2.43 |
| | Region | TRUE | 0.54 |
| | Division | FALSE | 0.20 |
| | State | TRUE | 0.10 |
| | County | FALSE | 0.25 |
| | Tract | TRUE | 0.10 |
| | Block Group | FALSE | 0.20 |
| | Block | TRUE | 0.10 |
| | Place | FALSE | 0.54 |
| | AIANNH | FALSE | 0.10 |
| | Total epsilon budget for P30: | | 3.27 |

## 3. Set Truncation Thresholds




## Error for P30

| | Region type | Selected | Total epsilon | Level | | Cell description | | MOE |
|---|---|---|---|---|---|---|---|---|
| 65 | USA | YES | 0.00 | 0 | Total: | | | 145.20 |
| 66 | USA | YES | 2.19 | 1 | | In married couple household | | 72.60 |
| 67 | USA | YES | 0.00 | 2 | | | Opposite-sex married couple | - |
| 68 | USA | YES | 0.00 | 2 | | | Same-sex married couple | - |
| 69 | USA | YES | 2.19 | 1 | | In cohabiting couple household | | 72.60 |
| 70 | USA | YES | 0.00 | 2 | | | Opposite-sex cohabiting couple | - |
| 71 | USA | YES | 0.00 | 2 | | | Same-sex cohabiting couple | - |
| 72 | USA | YES | 2.19 | 1 | | Male householder, no spouse or partner present | | 72.60 |
| 73 | USA | YES | 0.00 | 2 | | | Living alone | - |
| 74 | USA | YES | 0.00 | 2 | | | Living with others | - |
| 75 | USA | YES | 2.19 | 1 | | Female householder, no spouse or partner present | | 72.60 |
| 76 | USA | YES | 0.00 | 2 | | | Living alone | - |
| 77 | USA | YES | 0.00 | 2 | | | Living with others | - |

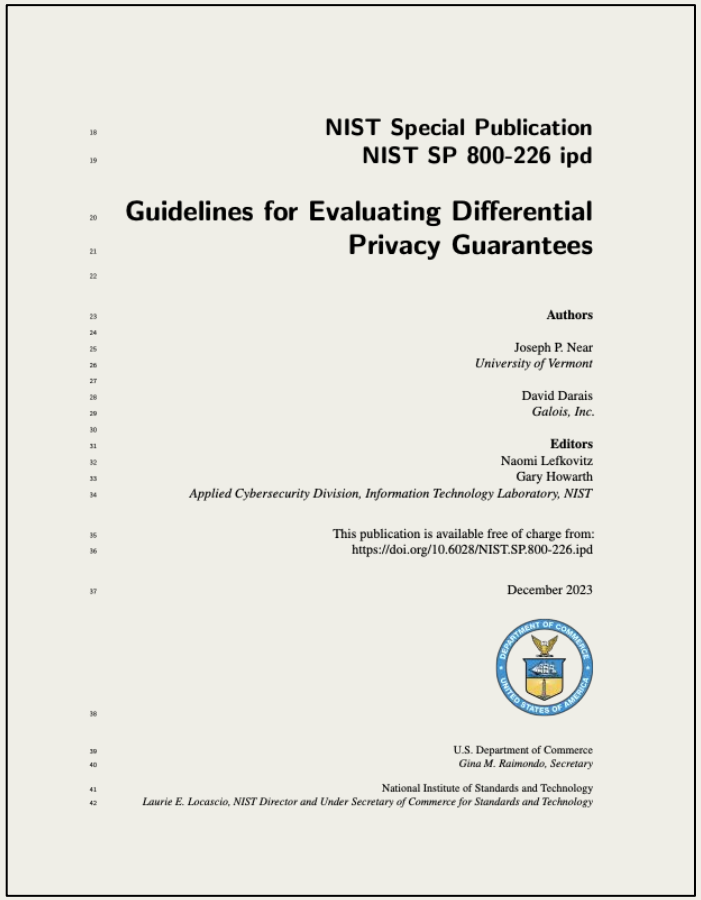
# Tune: Production Parameters for PHSafe

| Table | Truncation Threshold | Population Group Level | MOE Target | Unbounded Privacy Loss | Bounded Privacy Loss |
|---|---|---|---|---|---|
| PH1_num | 10 | (Nation, Unattributed) | 500 | 0.002619 | 0.005238 |
| | | (Nation, A-G) | 500 | 0.002619 | 0.005238 |
| | | (Nation, H-I) | 500 | 0.002619 | 0.005238 |
| | | (State, Unattributed) | 200 | 0.016371 | 0.032742 |
| | | (State, A-G) | 68 | 0.141622 | 0.283244 |
| | | (State, H-I) | 200 | 0.016371 | 0.032742 |
| PH1_denom | NA | (Nation, Unattributed) | 500 | 0.000022 | 0.000044 |
| | | (Nation, A-G) | 500 | 0.000022 | 0.000044 |
| | | (Nation, H-I) | 500 | 0.000022 | 0.000044 |
| | | (State, Unattributed) | 200 | 0.000135 | 0.00027 |
| | | (State, A-G) | 68 | 0.00117 | 0.00234 |
| | | (State, H-I) | 200 | 0.000135 | 0.00027 |
| PH2 | 10 | (Nation, Unattributed) | 500 | 0.002619 | 0.005238 |
| | | (State, Unattributed) | 200 | 0.016371 | 0.032742 |
| PH3 | 6 | (Nation, Unattributed) | 500 | 0.001061 | 0.002122 |
| | | (Nation, A-G) | 500 | 0.001061 | 0.002122 |
| | | (Nation, H-I) | 500 | 0.001061 | 0.002122 |
| | | (State, Unattributed) | 200 | 0.006630 | 0.01326 |
| | | (State, A-G) | 20 | 0.662976 | 1.325952 |
| | | (State, H-I) | 200 | 0.006630 | 0.01326 |

# Outline

- Designing PHSafe
- Tuning PHSafe
- **Deploying PHSafe**

## NIST strongly recommends using well-tested DP libraries



NIST Special Publication
NIST SP 800-226 ipd

# Guidelines for Evaluating Differential Privacy Guarantees


**Authors**

Joseph P. Near
*University of Vermont*

David Darais
*Galois, Inc.*

**Editors**
Naomi Lefkovitz
Gary Howarth
*Applied Cybersecurity Division, Information Technology Laboratory, NIST*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-226.ipd

December 2023



U.S. Department of Commerce
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*


**Privacy Hazard** Avoid custom implementations of differentially private algorithms, and use well-tested libraries instead.

**Privacy Hazard** Implementing differential privacy mechanisms is tricky and requires considering side-channel vulnerabilities.

**Privacy Hazard** When bounding user contributions, additional noise must be added to ensure user-level privacy.

**Privacy Hazard** In differentially private histograms, the analyst must specify the histogram bins. Otherwise, the presence or absence of a bin may leak information that violates differential privacy.

```
session = Session.from_dataframe(
    dataframe=private_data,
    source_id="my_data",
    RhoZCDPBudget(1.5)
)

query = (
    QueryBuilder("my_data")
    .filter("age < 18")
    .groupby(states)
    .count()
)

result = session.evaluate(
    query,
    RhoZCDPBudget(0.2)
)

print(session.remaining_privacy_budget())
# prints RhoZCDPBudget(1.3)
```

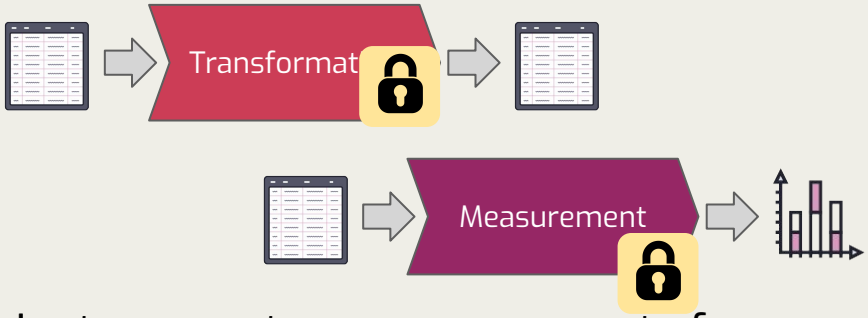
# Tumult Analytics

Intended for data scientists

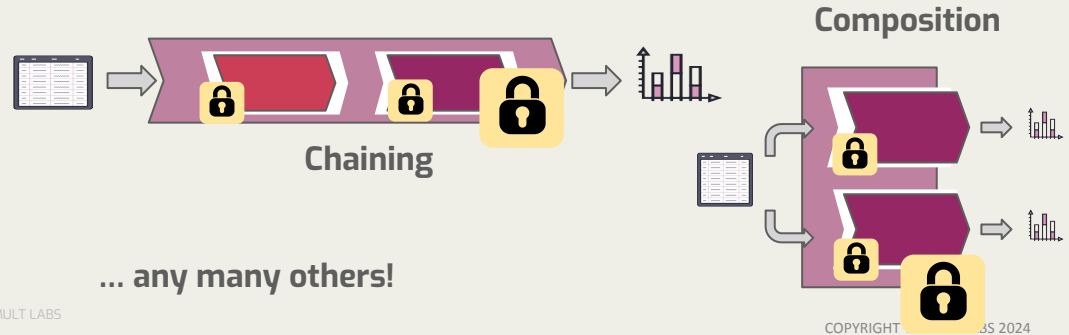
- DP expertise *not* required
- Python interface similar to pandas/spark

# Tumult **Core**

A collection of composable components: transformations and measurements.




Combinators create new components from existing ones.




Core enables creation of complex algorithms from building blocks

Everything carries an explicit, inspectable privacy guarantee 🔒

Every DP computation in core comes with a proof of privacy

# Conclusion

- What is PHSafe? S-DHC's privacy protection algorithm.

- Development workflow for deploying DP
  - How does PHSafe work?.....**Algorithm designed by privacy experts**
  - When does PHSafe work well?.....**Algorithm tuned by subjected-matter experts**
  - Why does PHSafe work?.....**Algorithm deployed on Tumult Analytics**