BPD Thinking Privacy

Swapnil
Mona

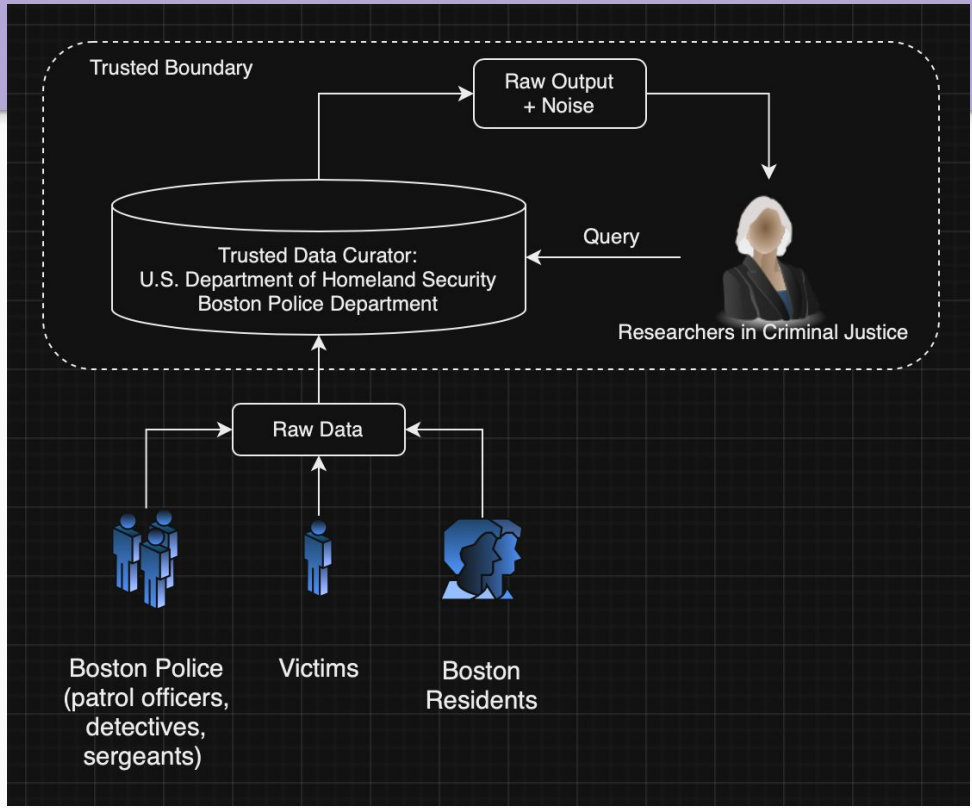
System Diagram

Trusted Data Curator: Access to aggregated and anonymized data, operational data including officer conduct records.

Untrusted Data Curator:
1) Boston Police - Access to data relevant to their own cases with restricted access to victim/resident's personal information

2) Victims - Access to their own case information without access to other victim's data or unrelated police operations.

3) Boston Residents: Access to public safety information and crime stats, but no sensitive data.



DP version of BPD

Where to add noise: To aggregate queries, for example:

- Total number of allegations across all police in the BPD.
- Total number of allegations for each neighborhood.
- Average response time to incidents by neighborhood or type of incident.

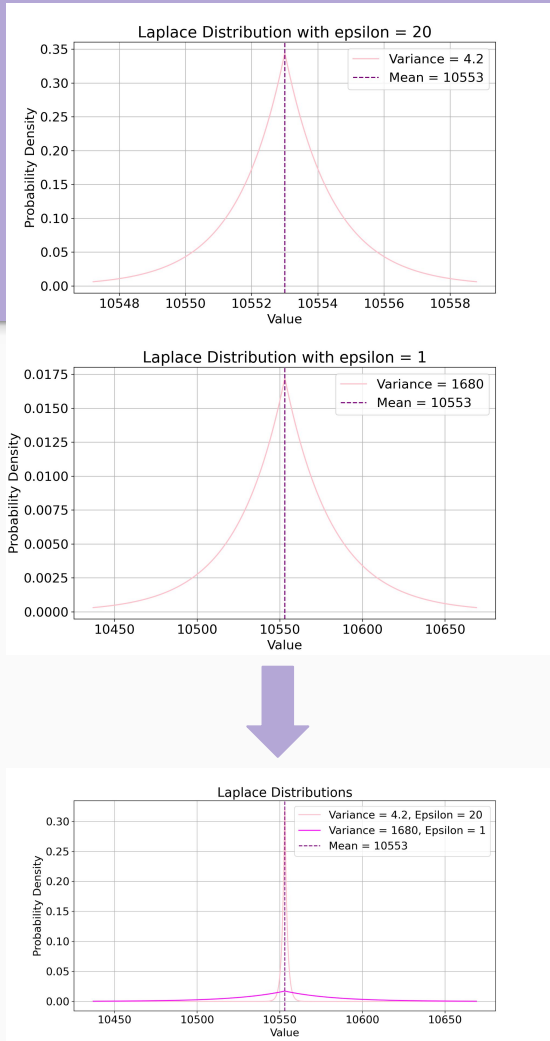
Which mechanism: Central Differential Privacy, Laplace mechanism

Why:

- Better accuracy with lower privacy.
- Striving for transparency to inform safety decisions while considering privacy.

Error Example: Sum Query

- Total number of allegations across all police in the Boston police department
- Sensitivity: 29 (if removing the 1st place)
- Use a Laplace mechanism, the noise: 10553+noise
- The maximum absolute error (variance) of our noisy answer: 2 (GS(q)/e)^2) = 2*29^2/e^2 = 1682/e^2
- Error: **~4.2 (e=20)**, **~1682 (e=1)** -> final count in the range of (10450, 10650)



Accuracy vs. Privacy

- Choose a large epsilon to minimize variance (error)
- Preserving basic human rights, especially in law enforcement data.

Current assumptions (will be adjusted based on future experiments):

- BPD collected info is uploaded every week
- Our epsilon: ~20
- Refresh Frequency: multiple weeks

Thank you for listening!

Any question?