Differential Private System for Boston Police Department (BPD) Dataset

Swapnil Gupta, Mona Ma

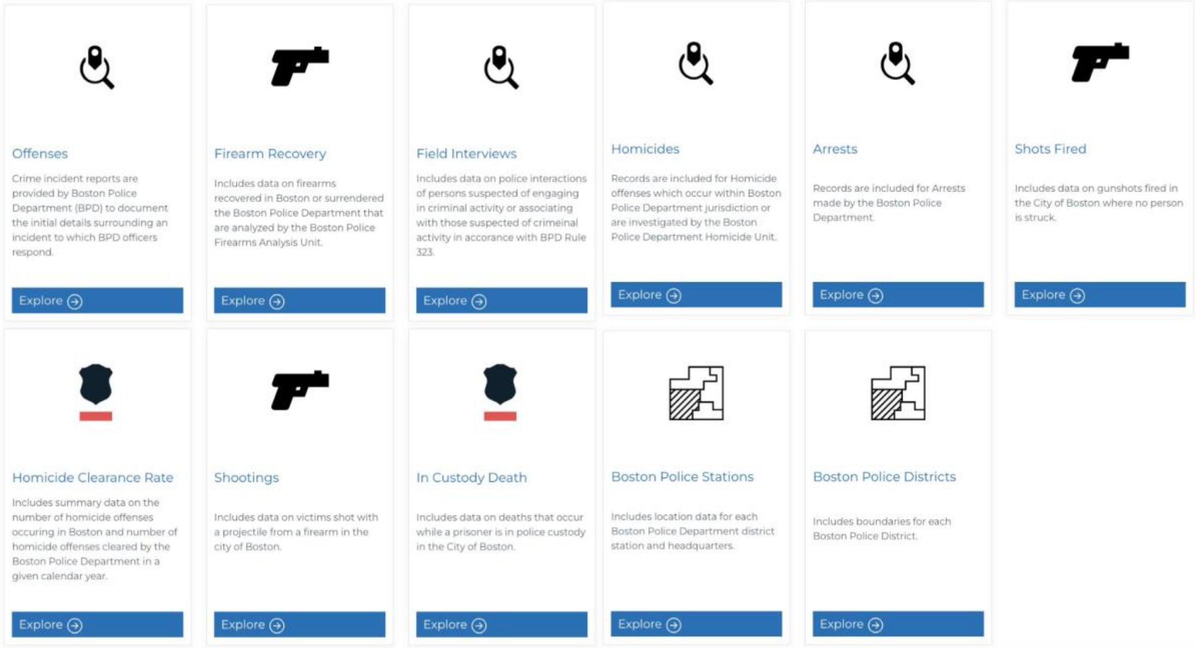
1. Abstract

We designed a differential privacy system for the Boston Police Department Dataset, incorporating data from three unique sources. By employing Central Differential Privacy (CDP) [10] and the Laplace Distribution [3], our system was implemented using SmartNoise [11], a tool developed by the OpenDP [12] community. We tested, fine-tuned, and allocated precise privacy budgets to each of the five representative queries, aiming to reduce error and enhance accuracy and transparency when noise was added to the aggregated outputs. Furthermore, our research explored side-channel attacks [2], with a focus on developing strategies to mitigate time leakage attacks [2].

2. Results

2.1 Dataset Presentation

Our dataset encompasses a wide range of information relevant to public safety, crime trends and law enforcement activities in Boston from three different datasets - "Boston Police Department Crime Hub Data [7]", "The Woke Windows Project [8]", and "Boston Cop Track [9]". It also includes information about allegations against Boston Police Department employees and a list of civilian and officer employees.



Offenses

Crime incident reports are provided by Boston Police Department (BPD) to document the initial details surrounding an incident to which BPD officers respond.

Firearm Recovery

Includes data on firearms recovered in Boston or surrendered the Boston Police Department that are analyzed by the Boston Police Firearms Analysis Unit.

Field Interviews

Includes data on police interactions of persons suspected of engaging in criminal activity or associating with those suspected of crimeinal activity in accorance with BPD Rule 323.

Homicides

Records are included for Homicide offenses which occur within Boston Police Department jurisdiction or are investigated by the Boston Police Department Homicide Unit.

Arrests

Records are included for Arrests made by the Boston Police Department.

Shots Fired

Includes data on gunshots fired in the City of Boston where no person is struck.

Homicide Clearance Rate

Includes summary data on the number of homicide offenses occuring in Boston and number of homicide offenses cleared by the Boston Police Department in a given calendar year.

Shootings

Includes data on victims shot with a projectile from a firearm in the city of Boston.

In Custody Death

Includes data on deaths that occur while a prisoner is in police custody in the City of Boston.

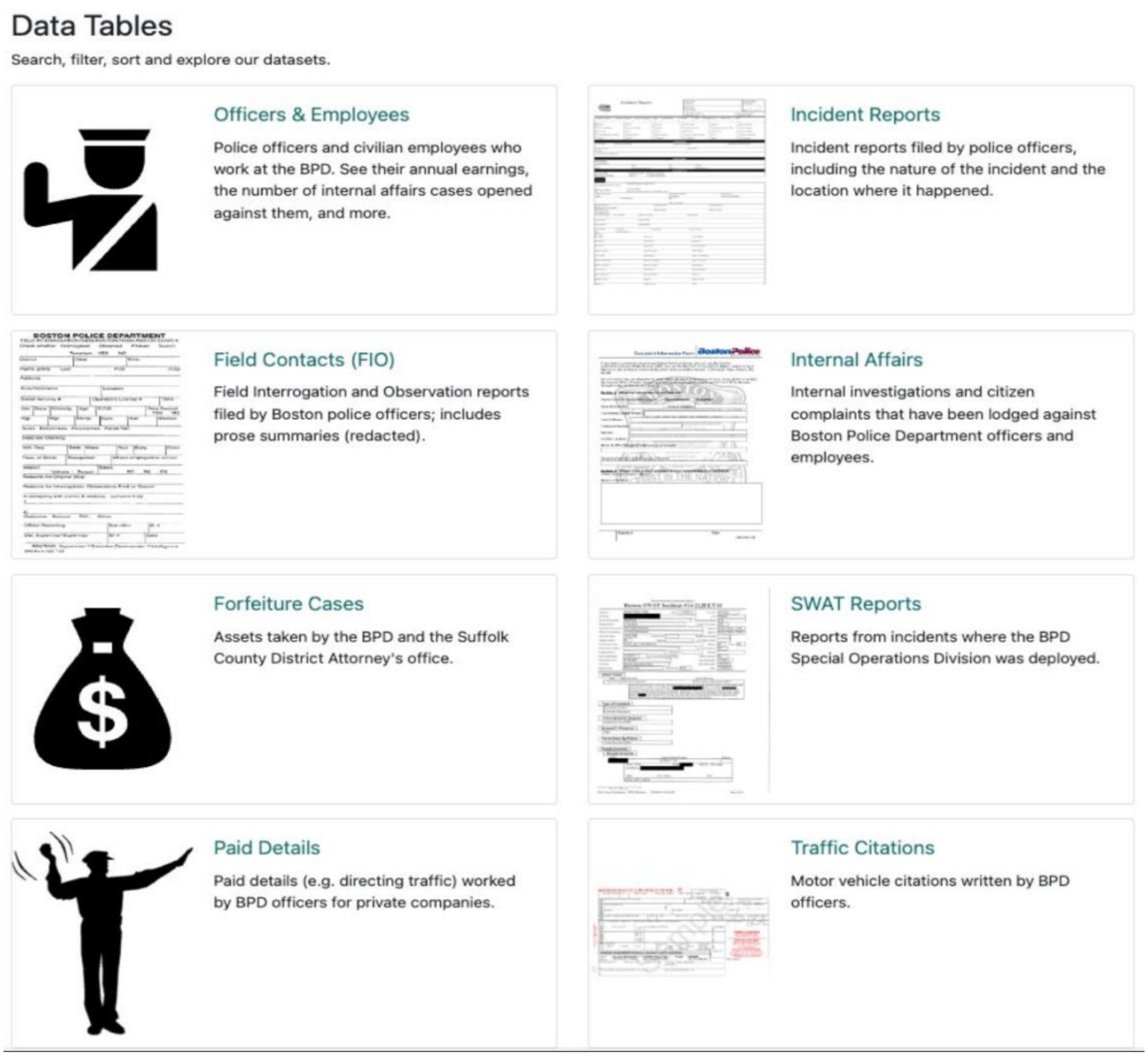
Boston Police Stations

Includes location data for each Boston Police Department district station and headquarters.

Boston Police Districts

Includes boundaries for each Boston Police District.

Figure 1.



Data Tables

Search, filter, sort and explore our datasets.

Officers & Employees

Police officers and civilian employees who work at the BPD. See their annual earnings, the number of internal affairs cases opened against them, and more.

Incident Reports

Incident reports filed by police officers, including the nature of the incident and the location where it happened.

Field Contacts (FIO)

Field Interrogation and Observation reports filed by Boston police officers; includes prose summaries (redacted).

Internal Affairs

Internal investigations and citizen complaints that have been lodged against Boston Police Department officers and employees.

Forfeiture Cases

Assets taken by the BPD and the Suffolk County District Attorney's office.

SWAT Reports

Reports from incidents where the BPD Special Operations Division was deployed.

Paid Details

Paid details (e.g. directing traffic) worked by BPD officers for private companies.

Traffic Citations

Motor vehicle citations written by BPD officers.

Figure 2.

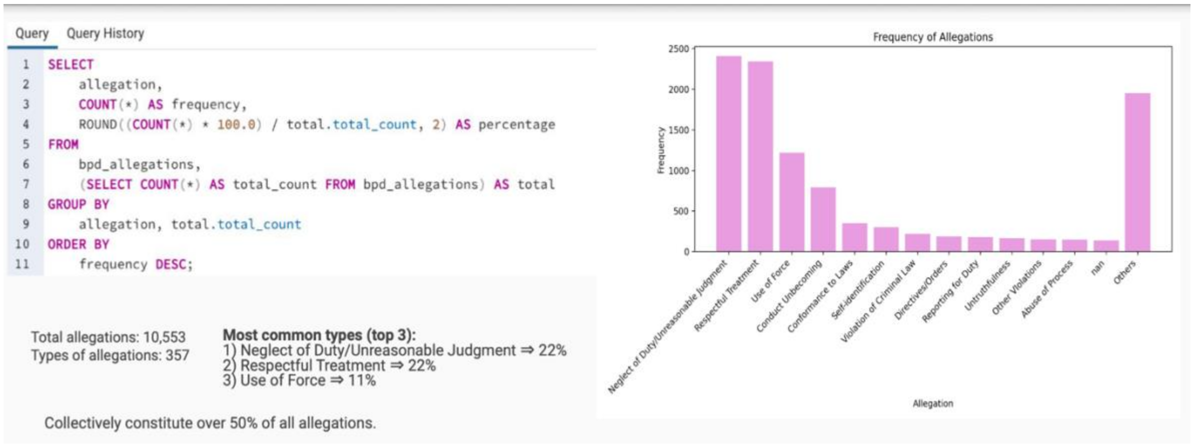
Our motivation for choosing this dataset is to analyze incidents involving the police, such as officer misconduct and several shootings that happened in Boston and its neighborhood, so as to enhance transparency and accountability within the department.

The dataset involves various stakeholders such as police departments, victims, and neighborhoods. Key privacy concerns include the potential misuse of sensitive police data, which could lead to targeted harassment or compromise internal security, as well as the possibility that neighborhood-level crime data might negatively impact public perceptions and community-police relations. Despite these challenges, our goal is to foster transparency, providing the community with essential information to improve their safety while diligently safeguarding individual privacy.

2.2 Running Analytics

We ran the following 3 different types of analytics on our dataset:

1. Different types of allegations and their frequencies.



```
SELECT
    allegation,
    COUNT(*) AS frequency,
    ROUND((COUNT(*) * 100.0) / total.total_count, 2) AS percentage
FROM
    bpd_allegations,
    (SELECT COUNT(*) AS total_count FROM bpd_allegations) AS total
GROUP BY
    allegation, total.total_count
ORDER BY
    frequency DESC;
```

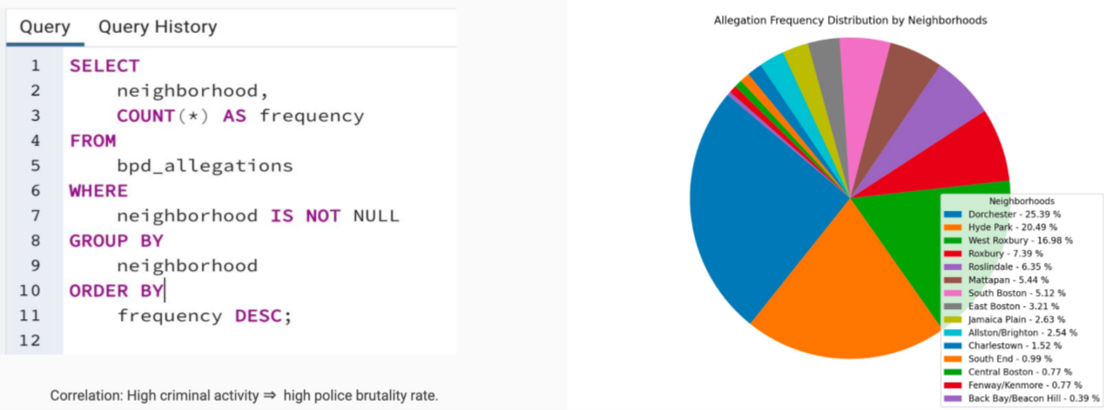
Total allegations: 10,553
Types of allegations: 357

Most common types (top 3):
1) Neglect of Duty/Unreasonable Judgment ⇒ 22%
2) Respectful Treatment ⇒ 22%
3) Use of Force ⇒ 11%

Collectively constitute over 50% of all allegations.

Figure 3.

2. The total number of allegations raised per neighborhood.



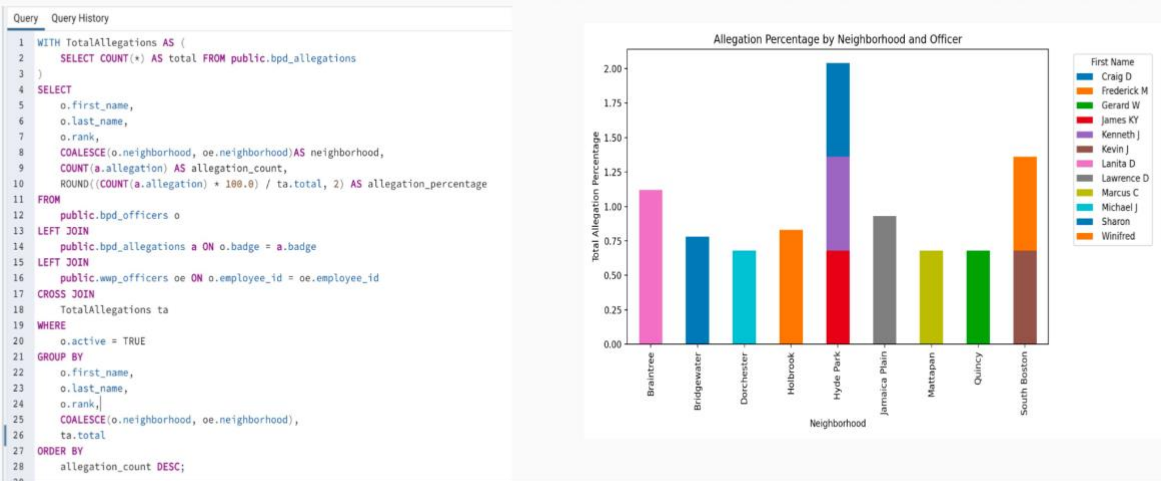
```
SELECT
    neighborhood,
    COUNT(*) AS frequency
FROM
    bpd_allegations
WHERE
    neighborhood IS NOT NULL
GROUP BY
    neighborhood
ORDER BY
    frequency DESC;
```

Correlation: High criminal activity ⇒ high police brutality rate.

Figure 4.

Dorchester, Hyde Park and West Roxbury are the 3 top most neighborhoods where allegations are raised against police officers.

3. The total number of allegations raised against each active police officer in various neighborhoods where they work.



```
WITH TotalAllegations AS (
    SELECT COUNT(*) AS total FROM public.bpd_allegations
)
SELECT
    o.first_name,
    o.last_name,
    o.rank,
    COALESCE(o.neighborhood, oe.neighborhood)AS neighborhood,
    COUNT(a.allegation) AS allegation_count,
    ROUND((COUNT(a.allegation) * 100.0) / ta.total, 2) AS allegation_percentage
FROM
    public.bpd_officers o
LEFT JOIN
    public.bpd_allegations a ON o.badge = a.badge
LEFT JOIN
    public.wwp_officers oe ON o.employee_id = oe.employee_id
CROSS JOIN
    TotalAllegations ta
WHERE
    o.active = TRUE
GROUP BY
    o.first_name,
    o.last_name,
    o.rank,
    COALESCE(o.neighborhood, oe.neighborhood),
    ta.total
ORDER BY
    allegation_count DESC;
```

Figure 5.

Out of 10553 allegations, Officer Lanita D. himself comprises around 59 (1.12%) of the total allegations raised.

Our stakeholders should take the following actions based on the above results:

1. Develop specialized training for officers to improve interactions and handle crises.
2. Revise and enforce clear operational policies to ensure accountability and transparency in policing practices.
3. Actively engage with the community through regular dialogue and targeted interventions in high-need areas like Dorchester and Hyde Park, fostering trust and understanding.

2.3 Thinking Privacy

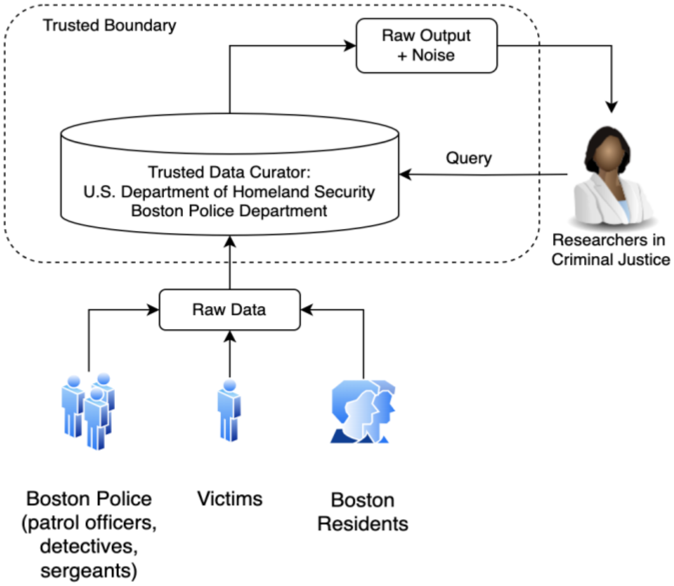

Trusted Boundary
Raw Output + Noise
Query
Trusted Data Curator:
U.S. Department of Homeland Security
Boston Police Department
Researchers in Criminal Justice
Raw Data
Boston Police (patrol officers, detectives, sergeants)
Victims
Boston Residents

Figure 6.

Only the Data Curator is trusted with access to the raw data. All other stakeholders are not trusted and receive limited access based on their roles. For each stakeholder, access should be granted according to the principle of least privilege: they should have access only to the data necessary to fulfill their roles or duties [6].

We aim to add noise to aggregate query results, and Central Differential Privacy (CDP) [10] is the best choice. We want to provide information as transparently as possible while also taking privacy into consideration. By using CDP [10], we can achieve better accuracy, helping residents and the BPD make well-informed decisions on issues related to public safety.

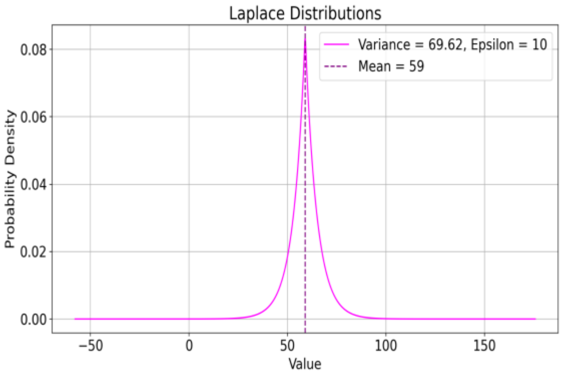


Figure 7.

The Laplace mechanism helps us calculate the error [3]. For instance, if we want to generate a CDP version of the total number of allegations across all police in the BPD, setting the privacy budget to 10 for this query results in an absolute error of 8.34 (with a variance of 69.62). This is acceptable because it does not significantly change the rankings of the police.

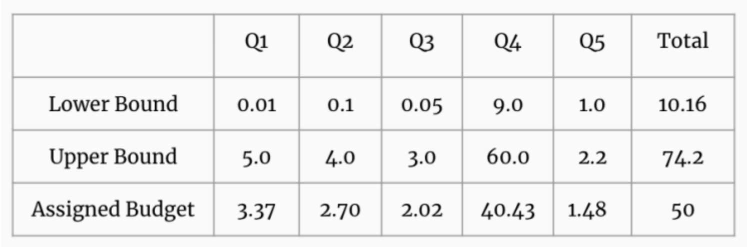
We plan to choose a large epsilon for each query to minimize error. Although we will lose some randomness in the aggregated results, it's crucial to make the results as transparent as possible while preserving privacy. Currently, the salaries, ages, and ranks of police officers, along with other sensitive information about victims, are all exposed. We want to preserve our stakeholders' privacy while making use of the available datasets.

2.4 Implementation

We implemented our design across five queries:

1. Different types of allegations and their frequencies.
2. The total number of allegations raised per neighborhood.
3. The total number of allegations raised against each active police officer.
4. The average salaries by rank or title of the officers.
5. The frequency of gunshots in different neighborhoods.

Here are the lower and upper bounds we summarized, along with the final assigned privacy budget:



	Q1	Q2	Q3	Q4	Q5	Total
Lower Bound	0.01	0.1	0.05	9.0	1.0	10.16
Upper Bound	5.0	4.0	3.0	60.0	2.2	74.2
Assigned Budget	3.37	2.70	2.02	40.43	1.48	50

Figure 8.

First, we decided to allocate a privacy budget of 10 per query evenly, but then we experimented with different epsilon values. The empirical results showed us these reasonable query ranges. Here are the plots for "epsilon versus errors" and "epsilon versus runtime":

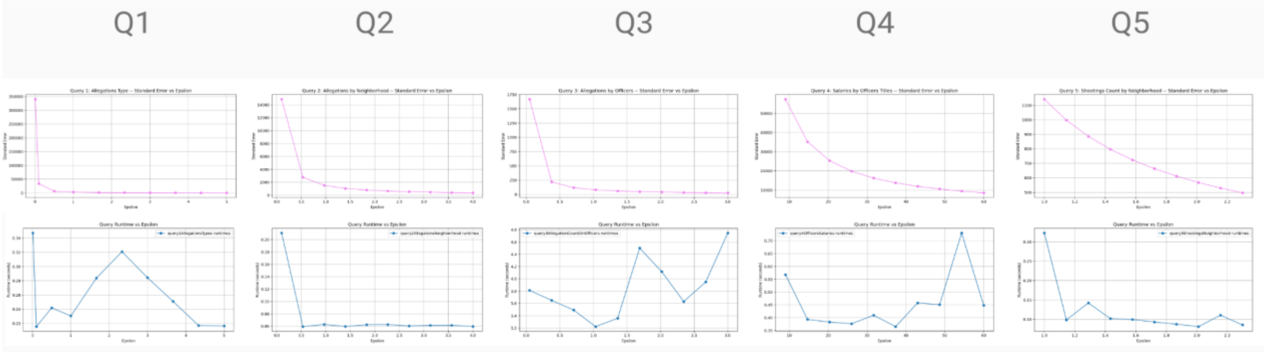


Figure 9.

Each query has a different range of epsilons based on its sensitivity. The error can change drastically with a small change in epsilon if the sensitivity is low. For Q3, with a sensitivity of 59 allegation counts by officers, we had to narrow the range of epsilon so that the added noise would be useful. For Q4, with a sensitivity of over 360,000 in the yearly income grouped by officers' titles, a greater epsilon range is necessary. The shared pattern here confirms with what we learned: the privacy budget is inversely related to expected noise [4]. As epsilon increases, the error decreases. This makes sense because, with loose budgets, we get results that are closer to the true value. The runtimes we got tend to be random for each run.

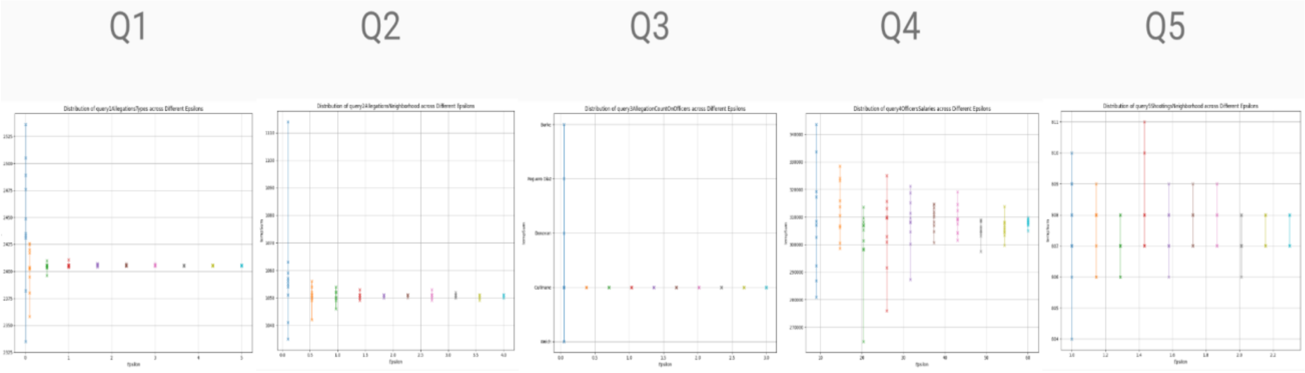


Figure 10.

The challenge here is to determine the reasonable range of epsilons for each query. As epsilon increases, the distribution of noised values should converge to the true value [1]. Initially, we did not observe this pattern because the values of epsilon were so large that they had already converged, even across multiple executions, therefore producing the same results—a single overlapped point rather than a randomized Laplace distribution [3]. Once we adjusted our selection based on the actual output of the noised results, we identified the reasonable range of epsilons for each query.

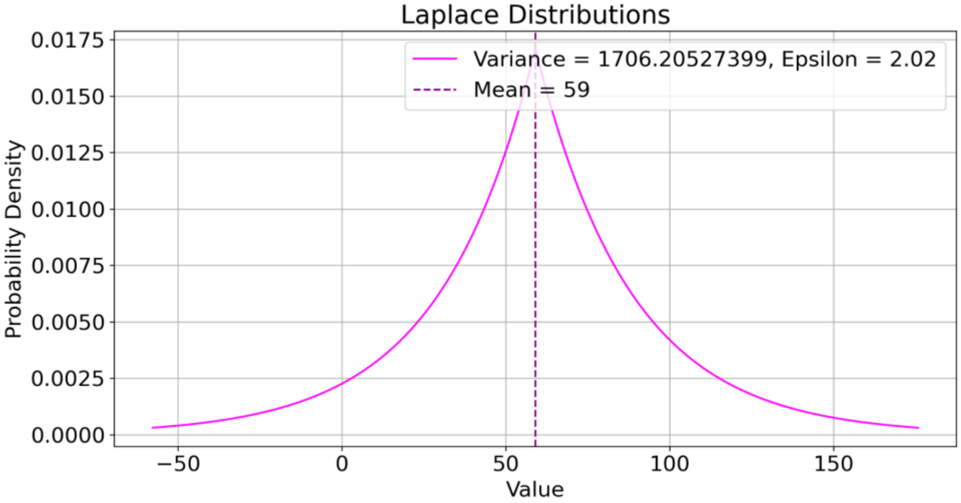


Figure 11.

Compared to Checkpoint 3, Thinking Privacy, where we initially used an epsilon of 10, we decided to assign a 2.02 privacy budget to Example Query 3. We want the aggregated result to be as precise as possible, yet with reasonable noise added. A smaller epsilon value corresponds to larger errors, but these errors do not significantly change the rankings. Thus, we chose a stricter epsilon value for this query.

2.5 Side Channels

Our system is vulnerable to timing leakage attacks. For example, the processing time of a query can reveal to hackers the proportion of police officers who hold the rank of 'patrol officer' (ptl) relative to the total number of Boston police. We demonstrated this by comparing the runtime of our original query to the same query with a WHERE clause (and rank = 'ptl') for the averages of 10 and 20 executions.

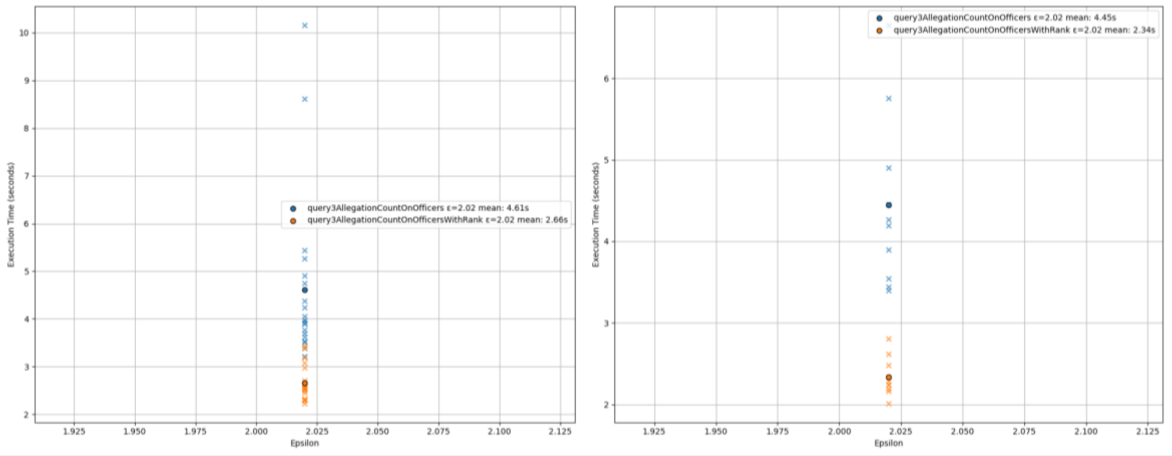


Figure 12.

Ten executions yielded a result of 52.6 percent, and twenty executions produced a result of 57.7 percent, whereas the true percentage of patrol officers was 54.3, based on the rows affected. The results are already close to the actual value. With more executions, it is possible to get a more accurate result.

One of the papers we read described four approaches to the timing-channel problem [2]. We decided to adopt a mechanism similar to the variable time approach: adding random delays within a tunable range of seconds to the response times of the queries.

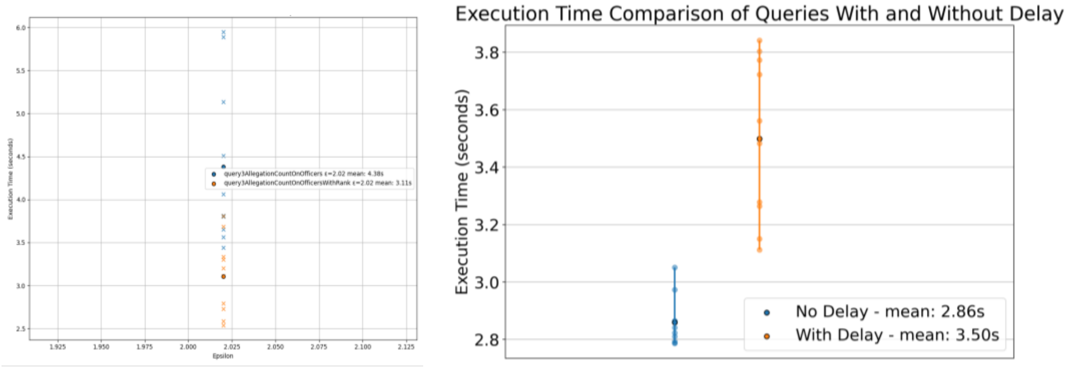


Figure 13.

For this query, we chose a range of delays from 4 to 21 percent, corresponding to delays of 0.1 to 0.5 seconds. The runtime comparison shows that the patrol officers are about 71 percent, which deviates from the true value. We also compared the runtime of running the original query with and without delays. Over 10 executions, the average delay was about 0.64 seconds. Since our database is relatively small, with a total of 15,000 entries, a delay of less than one second is completely acceptable. More importantly, this delay can be adjusted by the users based on the trade-off between performance and privacy guarantees.

3. What we learned from our analysis

Designing a differentially private version of a real-world dataset is not an easy task. We always questioned ourselves: Is it necessary to add noise to the results? For Query 5 in section 2.4, we chose to add noise to the frequency of gunshots in different neighborhoods because there are two areas where each has only one incident involving gunshots in the past five years. It’s easy for people to investigate and find private information about the victims and officers involved. Therefore, we added noise but still kept the rankings relatively the same to help people make informed decisions.

For Query 4 in section 2.4, which aggregates the average salaries grouped by the rank of the officers, the raw data itself simply exposed every police officer's income, without even anonymizing their names. Previously, we believed that each individual deserves the right to keep their salary confidential. However, with more research [13], we realized that public employees' salaries are disclosed as public records in the United States. Many other countries, including Canada, the UK, and Australia, have similar transparency laws regarding salary disclosure. This was definitely a cultural shock for us because China and India do not have this level of transparency regarding government workers' salaries. If given more time, we would shift our focus to identifying records that reveal victims' private information.

When we first chose the Boston Police Department datasets, we were simply inspired by the Chicago police dataset and hoped to find data sources more relevant to our daily lives. Although this dataset is not perfect and involves some gender and racial issues (for some of the tables, we don’t understand the purpose of exposing the victims' gender or ethnic information), it is still worth investigating for public safety and the privacy of the individuals involved.

Open Question:

Long-Term Data Management: Given the changes in legal frameworks over time, what are the best practices for managing older datasets that were collected under different assumptions about privacy and transparency? This is especially relevant as public perceptions and legal standards evolve.

4. References

[1] Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 9(3–4), 211-407.

[2] Haeberlen, A., Pierce, B. C., & Narayan, A. (2011). Differential privacy under fire. In 20th USENIX Security Symposium (USENIX Security 11).

[3] Hsu, J., Gaboardi, M., Haeberlen, A., Khanna, S., Narayan, A., Pierce, B. C., & Roth, A. (2014, July). Differential privacy: An economic method for choosing epsilon. In 2014 IEEE 27th Computer Security Foundations Symposium (pp. 398-410). IEEE.

[4] Nanayakkara, P., Bater, J., He, X., Hullman, J., & Rogers, J. (2022). Visualizing privacy-utility trade-offs in differentially private data releases. arXiv preprint arXiv:2201.05964.

[5] Gaboardi, M., Hay, M., & Vadhan, S. (2020, May 11). A Programming Framework for OpenDP. In Harvard University, Open Differential Privacy (OpenDP) Programming Framework White Paper

[6] Porter, A. (2023, March 9). Maximizing Data Security: Least Privilege Access. BigID. https://bigid.com/blog/maximizing-data-security-least-privilege-access/

[7] Boston Police Department (accessed May 2024). Boston Police Department Crime Hub Data.
https://boston-pd-crime-hub-boston.hub.arcgis.com/pages/data

[8] Story, Nathan (2021, April). The Woke Windows Project
https://www.wokewindows.org/

[9] Wolfinger, Matt (2022, January). Boston Cop Track data
https://mattewolfinger.github.io/resources.html

[10] Bater, J. (2024, February 28). Privacy vs accuracy [Slides]. Retrieved from
https://canvas.tufts.edu/courses/54828/files/folder/lectures?preview=7178845

[11] Smart Noise Documentation (2023). SmartNoise SQL.
https://docs.smartnoise.org/

[12] OpenDP Documentation (2023).
https://opendp.org/

[13] U.S. Census Bureau. (2022). Annual Survey of Public Employment & Payroll.
https://www.census.gov/programs-surveys/aspep.html

[14] Github Link:
https://github.com/MonaMaNotAvailable/BostonPoliceDataAnalysis-CS151DataPrivacySecurity

5. Contributions of each team member

5.1 Dataset Presentation

- Swapnil: Researched different datasets and wrote descriptions
- Mona: Explained why we chose the dataset
- Both: Came up with privacy concerns

5.2 Running Analytics

- Swapnil: Wrote 3 SQL queries
- Mona: Made visualizations
- Both: Wrote call to action

5.3 Thinking Privacy

- Swapnil: Designed DP System
- Mona: Calculated errors
- Both: Drawn system diagram & analyzed accuracy

5.4 Implementation

- Swapnil: Implemented and taught Mona how to use SmartNoised
- Mona: Wrote 2 SQL queries
- Both: Adjusted privacy budgets and created plots

5.5 Side Channels

Both of us did the following:

- Researched different leakage attacks and came up with Time leakage for our system
- Came up with the best possible query for time leakage for the system, and implemented the side channel
- Created the prevention strategy for the side channel attack by introducing random delays.
- All the analysis related to run time.